

# Variability Abstractions: Trading Precision for Speed in Family-Based Analyses

Extended Version <sup>\*</sup>

Aleksandar S. Dimovski, Claus Brabrand, and Andrzej Wąsowski

IT University of Copenhagen, Denmark

**Abstract.** Family-based (lifted) data-flow analysis for Software Product Lines (SPLs) is capable of analyzing all valid products (variants) without generating any of them explicitly. It takes as input only the common code base, which encodes all variants of a SPL, and produces analysis results corresponding to all variants. However, the computational cost of the lifted analysis still depends inherently on the number of variants (which is exponential in the number of features, in the worst case). For a large number of features, the lifted analysis may be too costly or even infeasible. In this paper, we introduce variability abstractions defined as Galois connections and use abstract interpretation as a formal method for the calculational-based derivation of approximate (abstracted) lifted analyses of SPL programs, which are sound by construction. Moreover, given an abstraction we define a syntactic transformation that translates any SPL program into an abstracted version of it, such that the analysis of the abstracted SPL coincides with the corresponding abstracted analysis of the original SPL. We implement the transformation in a tool, **reconfigurator** that works on Object-Oriented Java program families, and evaluate the practicality of this approach on three Java SPL benchmarks.

## 1 Introduction and Motivation

Software Product Lines (SPLs) are an effective strategy for developing and maintaining a family of related programs. Any valid program (*variant*) of an SPL is specified in terms of features selected. A *feature* is a distinctive aspect, quality, or characteristic from the problem-domain of a system. SPLs have been adopted by the industry because of improvements in productivity and time-to-market [7]. While there are many implementation strategies, many industrial product lines are implemented using annotative approaches such as conditional compilation; in particular, via the C-preprocessor `#ifdef` construct [15].

Recently, formal analysis and verification of SPLs have been a topic of considerable research (see [19] for a survey). The challenge is to develop analysis and verification techniques that work at the level of program families, rather than the level of individual programs. Given that the number of variants grows

---

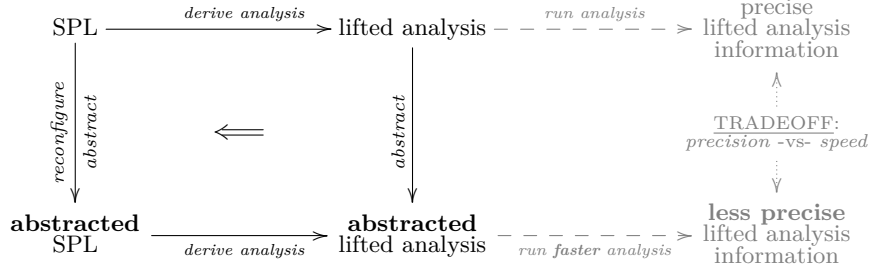
<sup>\*</sup> Partially supported by The Danish Council for Independent Research under a Sapere Aude project, VARIETE.

exponentially with the number of features, the need for efficient analysis and verification techniques is essential. To address this, a number of so-called *lifted* techniques have emerged, essentially lifting existing analysis and verification techniques to work on program families, rather than on individual programs. This includes lifted type checking [14], lifted data-flow analysis [5,4], lifted model checking [6]. They are also known as family-based (*variability-aware* or feature-sensitive) techniques. Lifted techniques are capable of analyzing the entire code base (all variants at once), without having to explicitly generate and analyze all individual variants, one at a time. Also, lifted techniques are capable of pin-pointing errors directly in the product line, as opposed to reporting errors in an individual product derived from the SPL.

There are two ways to speed up analyses: improving *representation* and increasing *abstraction*. The former has received considerable attention in the field of family-based analysis. In this paper, we investigate the latter. We consider a range of abstractions at the *variability level* that may tame the combinatorial explosion of configurations and reduce it to something more tractable by manipulating the configuration space of a program. Such variability abstractions enable deliberate trading of precision for speed in family-based analyses, even turn infeasible analyses into feasible ones, while retaining an intimate relationship back to the original analysis (via the abstraction).

We organize our variability abstractions in a calculus that provides convenient, modular, and compositional declarative specification of abstractions. We propose two basic abstraction operators (*project* and *join*) and two compositional abstraction operators (*sequential composition* and *parallel composition*). Each abstraction expresses a compromise between precision and speed in the induced abstracted analysis. We show how to apply each of these abstractions to data-flow lifted analyses, to extract (derive) their corresponding efficient and sound (correct) abstracted lifted analysis based on the calculational approach of abstract interpretation developed in [11]. Note that the approach is applicable to *any* analysis phrased as an abstract interpretation; in particular, it is not limited to data-flow analysis.

We observe that for variability abstractions, *analysis abstraction* and *analysis derivation* commute. Figure 1 illustrates how analysis abstraction is classically undertaken and how we propose to optimize it. The top left corner shows a product line that we want to analyze. A lifted analyzer will take an SPL as input and derive a “lifted analysis” (rightward arrow). We can then run that lifted analysis (next rightward dashed arrow) and obtain our “*precise* lifted analysis information”. (Note that for some analyzers, the phases *derive analysis* and subsequent *run analysis* may be so intertwined that they are not independently distinguishable.) Since running the analysis might be too slow or infeasible, we may decide to use abstraction to obtain a faster, although less precise analysis. Classically, an abstraction is applied to the derived analysis before it is run (middle arrow down) which, after an often long and complex process, produces an “abstracted lifted analysis”. When that analysis is subsequently run, it will



**Fig. 1.** Diagram illustrating the role and intended usage of the **reconfigurator** transformation. Instead of abstracting an already existing (or derived) lifted analysis, our transformation allows abstraction to be applied directly to the SPL. The resulting “abstracted SPL” can then be analyzed using existing techniques. The two paths from SPL to “abstracted lifted analysis” are guaranteed to produce the same abstracted lifted analysis.

produce less precise analysis information, but it will do so faster than the original analysis (i.e., there is a *precision vs. speed tradeoff*).

Interestingly, for lifted analyses and variability abstractions, the analysis abstraction (down) and derivation (right) commute and we may swap their order of application, as indicated by the short double leftward arrow in the center. The implications are quite significant. It means that variability abstractions can be applied *before*, and independently of, the subsequent analysis. This also means that the same variability abstractions might be applicable to all sorts of analyses that are specifiable via abstract interpretation; including, but not limited to: data-flow analysis [8], model checking [12], type systems [10] and testing [13].

We exploit this observation to define a *stand-alone* source-to-source transformation for programs with `#ifdefs`, implemented in a tool, **reconfigurator**. It takes an input SPL program and a variability abstraction and produces an abstracted SPL program such for which the subsequent lifted analysis agrees with “abstracted lifted analysis” of the original unabstracted SPL. Since the **reconfigurator** is based on a source-to-source transformation, and like a pre-processor it is essentially unaware of the programming language syntax, it can be used for any analysis. Many existing analysis methods that are unable to abstract variability benefit from this work instantly. Almost no extension or adaptation is required as the abstraction is applied to source code before analysis.

We evaluate our approach by comparing analyses of a range of increasingly abstracted SPLs against their origins without abstraction, quantifying to what extent precision can be traded for speed in lifted analyses.

In summary, the paper makes the following contributions:

- C1:** *Variability abstraction* as a method for trading precision for speed in family-based analysis (based on abstract interpretation);

- C2:** A *calculus* for modular specification of variability abstractions;
- C3:** The observation that certain analysis derivations and analysis abstractions *commute*, meaning that variability abstractions can be applied directly on an SPL *before* (and independently of) subsequent lifted analysis;
- C4:** A stand-alone *transformation*, **reconfigurator**, based on the above ideas;
- C5:** An *evaluation* of the above ideas; in particular, an evaluation of the tradeoff between precision and speed in family-based analyses.

We direct this work to program analysis and software engineering researchers. The method of *variability abstractions* (**C1–C3**) is directed at designers of lifted analyses for product lines. They may use our insights to design improved abstracted analyses that appropriately trade precision for speed. Note that the ideas apply beyond the context of data-flow analyses (e.g., to model checking, type systems, verification, and testing). The **reconfigurator** (**C4**) and the evaluation lessons (**C5**) are relevant for software engineers working on preprocessor-based product lines and who would like to speed up existing analyzers.

We proceed by introducing the basics of lifting analyses in Section 2. Section 3 defines a calculus for specification of variability abstractions. Section 4 explains how to apply an abstraction to a lifted analysis. It uses constant propagation as an example. The **reconfigurator** is described in Section 5 along with correctness for our example analysis. Section 6 presents the evaluation on three Java Object-Oriented SPLs. Finally, we discuss the relation to other works and conclude.

## 2 Program Families and Lifted Analyses

In this section we summarize the prerequisites for presenting our work. We define *features*, *configurations*, *feature expressions*, and a *feature model* which designates a set of *valid* configurations. Hereafter, we describe a simple imperative language IMP for writing program families. Finally, we briefly sketch a lifted constant propagation analysis for this language, formally derived in [17]. We focus on constant propagation for presentation purposes; our approach is generically applicable to any lifted analysis phrased as an abstract interpretation.

*Features, Configurations, and Feature Expressions.* Let  $\mathbb{F} = \{A_1, \dots, A_n\}$  be a finite set of *features*, each of which may be *enabled* or *disabled* in a particular program variant. A *feature expression*, *FeatExp* formula, is a propositional logic formula over  $\mathbb{F}$ , defined inductively by:

$$\varphi ::= A \in \mathbb{F} \mid \neg \varphi \mid \varphi_1 \wedge \varphi_2$$

A truth assignment or *valuation* is a mapping  $v$  assigning a truth value to all features. Every feature expression evaluates to some truth value under the valuation  $v$ . We say that  $\varphi$  is *valid*, denoted as  $\models \varphi$ , if  $\varphi$  evaluates to *true* for all valuations  $v$ . We say that  $\varphi$  is *satisfiable*, denoted as  $\text{sat}(\varphi)$ , if there exists a valuation  $v$  such that  $\varphi$  evaluates to *true* under  $v$ . We say that the formula  $\theta$  is a semantic consequence of  $\varphi$ , denoted as  $\varphi \models \theta$ , if for all satisfiable valuations  $v$  of  $\varphi$  it follows that  $\theta$  evaluates to *true* under  $v$ . Otherwise, we have  $\varphi \not\models \theta$ .

*Feature Model.* A feature model describes the set of *valid* configurations (variants) of a product line in terms of features and relationships among them. For our purposes a feature model can be equated to a propositional formula [2], say  $\psi \in \text{FeatExp}$ , as the semantic aspects of feature models beyond the configuration semantics, are not relevant here. We write  $\mathbb{K}_\psi$  to denote the set of all *valid* configurations described by the feature model,  $\psi$ ; i.e., the set of all satisfiable valuations of  $\psi$ . One satisfiable valuation  $v$  represents a valid configuration, and it can be also encoded as a conjunction of literals:  $k_v = v(A_1) \cdot A_1 \wedge \dots \wedge v(A_n) \cdot A_n$ , where  $\text{true} \cdot A = A$  and  $\text{false} \cdot A = \neg A$ , such that  $k_v \models \psi$ . The truth value of a feature in  $v$  indicates whether the given feature is *enabled* (included) or *disabled* (excluded) in the corresponding configuration. Let  $k_{v_1}, \dots, k_{v_n}$  ( $1 \leq n \leq 2^{|\mathbb{F}|}$ ) represent all satisfiable valuations of  $\psi$  expressed as formulas, then  $\mathbb{K}_\psi = \{k_{v_1}, \dots, k_{v_n}\}$ . For example, the set of features,  $\mathbb{F} = \{A, B\}$ , and the feature model,  $\psi = A \vee B$ , yield the following set of *valid* configurations:  $\mathbb{K}_\psi = \{A \wedge B, A \wedge \neg B, \neg A \wedge B\}$ .

*The Programming Language.*  $\overline{\text{IMP}}$  is an extension of the imperative language IMP [21] often used in semantic studies.  $\overline{\text{IMP}}$  adds a compile-time conditional statement for encoding multiple variants of a program. The new statement “**#if** ( $\theta$ )  $s$ ” contains a feature expression  $\theta \in \text{FeatExp}$  as a condition and a statement  $s$  that will be run, i.e. included in a variant, iff the condition  $\theta$  is satisfied by the corresponding configuration  $k \in \mathbb{K}_\psi$ . The abstract syntax of the language is given by the following grammar:

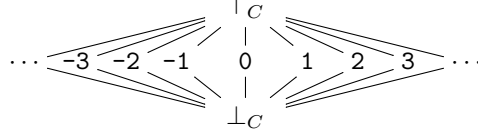
$$\begin{aligned} s &::= \text{skip} \mid \mathbf{x} := e \mid s ; s \mid \text{if } e \text{ then } s \text{ else } s \mid \text{while } e \text{ do } s \mid \text{\#if } (\theta) s \\ e &::= n \mid \mathbf{x} \mid e \oplus e \end{aligned}$$

where  $n$  ranges over integers,  $\mathbf{x}$  ranges over variable names  $\text{Var}$ , and  $\oplus$  over binary arithmetic operators. The set of all generated statements  $s$  (respectively expressions  $e$ ) is denoted by  $\text{Stm}$  (respectively  $\text{Exp}$ ). Notice that  $\overline{\text{IMP}}$  is only used for presentational purposes as a well established minimal language. Still, the introduced methodology is not limited to  $\overline{\text{IMP}}$  or its features. In fact, we evaluate our approach on Object-Oriented program families written in Java.

The semantics of  $\overline{\text{IMP}}$  has two stages. First, a preprocessor takes as input an  $\overline{\text{IMP}}$  program and a configuration  $k \in \mathbb{K}_\psi$ , and outputs a variant, i.e. an IMP program without **#if**-s, corresponding to  $k$ . All “**#if** ( $\theta$ )  $s$ ” statements are appropriately resolved in the generated valid product, i.e.  $s$  is included in it iff  $k \models \theta$ . Then, the obtained variant is executed (compiled) using the standard IMP semantics [21].

*Constant Propagation Analysis.* In the context of  $\overline{\text{IMP}}$  lifting means taking a static analysis that works on IMP programs, and transforming it into an analysis that works on  $\overline{\text{IMP}}$  programs, without preprocessing them (so on all the variants simultaneously). The lifted constant propagation analysis for IMP was derived in [17]. We first define a constant propagation lattice  $\langle \text{Const}, \sqsubseteq_C \rangle$ , whose partial

ordering  $\sqsubseteq_C$  is given by:



In this domain  $\top_C$  indicates a *non-constant* value, and  $\perp_C$  indicates *unanalyzed* information. All other elements indicate constant values. The partial ordering  $\sqsubseteq_C$  induces a least upper bound,  $\sqcup_C$ , and a greatest lower bound operator,  $\sqcap_C$ , on the lattice elements. For example, we have  $0 \sqcup_C 1 = \top_C$ ,  $\top_C \sqcap_C 1 = 1$ , etc.

The constant propagation analysis is given in terms of abstract *constant propagation stores*, denoted by  $a$ , essentially mappings of variables to elements of  $Const$ . Thus  $a(x)$  informs whether the variable  $x$  is a constant, and, in this case, what is its value. We write  $\mathbb{A} = Var \rightarrow Const$  meaning the domain of all constant propagation stores. Since  $Const$  is a complete lattice then so is  $\langle \mathbb{A}, \sqsubseteq_{\mathbb{A}}, \sqcup_{\mathbb{A}}, \sqcap_{\mathbb{A}}, \perp_{\mathbb{A}}, \top_{\mathbb{A}} \rangle$  obtained by point-wise lifting [21]. For example, for  $a, a' \in \mathbb{A}$  we have  $a \sqsubseteq_{\mathbb{A}} a'$  iff  $\forall x \in Var, a(x) \sqsubseteq_C a'(x)$ . We omit the subscripts  $C$  and  $\mathbb{A}$  whenever they are clear in context.

*Lifted Constant Propagation Analysis.* For the lifted constant propagation analysis, we work with the lifted property domain  $\langle \mathbb{A}^{\mathbb{K}_{\psi}}, \sqsubseteq, \sqcup, \sqcap, \perp, \top \rangle$ , where  $\mathbb{A}^{\mathbb{K}_{\psi}}$  is shorthand for the  $|\mathbb{K}_{\psi}|$ -fold product  $\prod_{k \in \mathbb{K}_{\psi}} \mathbb{A}$ , i.e. there is one separate copy of  $\mathbb{A}$  for each valid configuration of  $\mathbb{K}_{\psi}$ . The ordering  $\sqsubseteq$  is lifted configuration-wise; i.e., for  $\bar{a}, \bar{a}' \in \mathbb{A}^{\mathbb{K}_{\psi}}$  we have  $\bar{a} \sqsubseteq \bar{a}' \equiv_{def} \pi_k(\bar{a}) \sqsubseteq_{\mathbb{A}} \pi_k(\bar{a}')$  for all  $k \in \mathbb{K}_{\psi}$ . Here  $\pi_k$  selects the  $k^{\text{th}}$  component of a tuple. Similarly, we lift configuration-wise all other elements of the complete lattice  $\mathbb{A}$ , obtaining  $\sqcup, \sqcap, \perp, \top$ . E.g.,  $\top = \prod_{k \in \mathbb{K}_{\psi}} \top_{\mathbb{A}} = (\top_{\mathbb{A}}, \dots, \top_{\mathbb{A}})$ .

The lifted analysis  $\bar{\mathcal{A}}[s]$  should be a function from  $\mathbb{A}^{\mathbb{K}_{\psi}}$  to  $\mathbb{A}^{\mathbb{K}_{\psi}}$ . However, using a tuple of  $|\mathbb{K}_{\psi}|$  independent simple functions of type  $\mathbb{A} \rightarrow \mathbb{A}$  is sufficient. Thus, the lifted analysis is given by the function  $\bar{\mathcal{A}}[s] : (\mathbb{A} \rightarrow \mathbb{A})^{\mathbb{K}_{\psi}}$ , which represents a tuple of  $|\mathbb{K}_{\psi}|$  functions of type  $\mathbb{A} \rightarrow \mathbb{A}$ . The  $k$ -th component of  $\bar{\mathcal{A}}[s]$  defines the analysis corresponding to the valid configuration described by the formula  $k$ . Thus, an analysis  $\bar{\mathcal{A}}[s]$  transforms a lifted store,  $\bar{a} \in \mathbb{A}^{\mathbb{K}_{\psi}}$ , into another lifted store of the same type. For simplicity, we overload the  $\lambda$ -abstraction notation, so creating a tuple of functions looks like a function on tuples: we write  $\lambda \bar{a}. \prod_{k \in \mathbb{K}} f_k(\pi_k(\bar{a}))$  to mean  $\prod_{k \in \mathbb{K}} \lambda a_k. f_k(a_k)$ . Similarly, if  $\bar{f} : (\mathbb{A} \rightarrow \mathbb{A})^{\mathbb{K}}$  and  $\bar{a} \in \mathbb{A}^{\mathbb{K}}$ , then we write  $\bar{f}(\bar{a})$  to mean  $\prod_{k \in \mathbb{K}} \pi_k(\bar{f})(\pi_k(\bar{a}))$ .

The equations for lifted analysis  $\bar{\mathcal{A}}[s] : (\mathbb{A} \rightarrow \mathbb{A})^{\mathbb{K}_{\psi}}$  and  $\bar{\mathcal{A}}'[e] : (\mathbb{A} \rightarrow Const)^{\mathbb{K}_{\psi}}$  that analyse all valid configurations simultaneously are given in Fig 2. They are systematically derived in [17] by following the steps of the calculational approach to abstract interpretation [11]: define collecting semantics, specify a series of Galois connections and compose them with the collecting semantics to obtain the resulting analysis, which is thus sound (correct) by construction. Monotonicity of  $\bar{\mathcal{A}}[s]$  and  $\bar{\mathcal{A}}'[e]$  was shown in [17] as well.

$$\begin{aligned}
\overline{\mathcal{A}}[\text{skip}] &= \lambda \bar{a}. \bar{a} \\
\overline{\mathcal{A}}[\mathbf{x} := e] &= \lambda \bar{a}. \prod_{k \in \mathbb{K}_\psi} (\pi_k(\bar{a}))[\mathbf{x} \mapsto \pi_k(\overline{\mathcal{A}'}[e]\bar{a})] \\
\overline{\mathcal{A}}[s_0 ; s_1] &= \overline{\mathcal{A}}[s_1] \circ \overline{\mathcal{A}}[s_0] \\
\overline{\mathcal{A}}[\text{if } e \text{ then } s_0 \text{ else } s_1] &= \lambda \bar{a}. \overline{\mathcal{A}}[s_0]\bar{a} \dot{\cup} \overline{\mathcal{A}}[s_1]\bar{a} \\
\overline{\mathcal{A}}[\text{while } e \text{ do } s] &= \text{lfp } \lambda \bar{\Phi}. \lambda \bar{a}. \bar{a} \dot{\cup} \bar{\Phi}(\overline{\mathcal{A}}[s]\bar{a}) \\
\overline{\mathcal{A}}[\text{\#if } (\theta) s] &= \lambda \bar{a}. \prod_{k \in \mathbb{K}_\psi} \begin{cases} \pi_k(\overline{\mathcal{A}}[s]\bar{a}) & \text{if } k \models \theta \\ \pi_k(\bar{a}) & \text{if } k \not\models \theta \end{cases} \\
\overline{\mathcal{A}'}[n] &= \lambda \bar{a}. \prod_{k \in \mathbb{K}_\psi} n \\
\overline{\mathcal{A}'}[\mathbf{x}] &= \lambda \bar{a}. \prod_{k \in \mathbb{K}_\psi} \pi_k(\bar{a})(\mathbf{x}) \\
\overline{\mathcal{A}'}[e_0 \oplus e_1] &= \lambda \bar{a}. \prod_{k \in \mathbb{K}_\psi} \pi_k(\overline{\mathcal{A}'}[e_0]\bar{a}) \hat{\oplus} \pi_k(\overline{\mathcal{A}'}[e_1]\bar{a})
\end{aligned}$$

**Fig. 2.** Definitions of  $\overline{\mathcal{A}}[s] : (\mathbb{A} \rightarrow \mathbb{A})^{\mathbb{K}_\psi}$  and  $\overline{\mathcal{A}'}[e] : (\mathbb{A} \rightarrow \text{Const})^{\mathbb{K}_\psi}$ .

The (transfer) function  $\overline{\mathcal{A}}[s]$  captures the effect of analysing the statement  $s$  in an input store  $\bar{a}$  by computing an output store  $\bar{a}'$ . For the **skip** statement, the analysis function is an identity on lifted stores. For the assignment statement,  $\mathbf{x} := e$ , the value of variable  $\mathbf{x}$  is updated in every component of the input store  $\bar{a}$  by the value of the expression  $e$  evaluated in the corresponding component of  $\bar{a}$ . The **if** case results in the least upper bound (join) of the effects from the two corresponding branches, and it abstracts away the analysis information at the guard (condition) point. For the **while** statement, we compute the least fixed point of a functional<sup>1</sup> in order to capture the effect of running all possible iterations of the **while** loop. This fixed point exists and is computable by Kleene's fixed point theorem, since the functional is a monotone function over complete lattice with finite height [17,8]. For the **\#if**  $(\theta) s$  statement, we check for each valid configuration  $k$ <sup>2</sup> whether the feature constraint  $\theta$  is satisfied and, if so, it updates the corresponding component of the input store by the effect of evaluating the statement  $s$ . Otherwise, the corresponding component of the store is not updated. The function  $\overline{\mathcal{A}'}[e]$  describes the result of evaluating the expression  $e$  in a lifted store. Note that, for each binary operator  $\oplus$ , we define the corresponding

<sup>1</sup> The functional of the **while** rule is:  $\lambda \bar{\Phi}. \lambda \bar{a}. \bar{a} \dot{\cup} \bar{\Phi}(\overline{\mathcal{A}}[s]\bar{a})$ .

<sup>2</sup> Since any  $k \in \mathbb{K}_\psi$  is a valuation, we have that  $k \not\models \theta$  and  $k \models \neg\theta$  are equivalent for any  $\theta \in \text{FeatExp}$ .

constant propagation operator  $\hat{\oplus}$ , which operates on values from  $Const$ , as follows:

$$v_0 \hat{\oplus} v_1 = \begin{cases} \perp & \text{if } v_0 = \perp \vee v_1 = \perp \\ \mathbf{n} & \text{if } v_0 = \mathbf{n}_0 \wedge v_1 = \mathbf{n}_1, \text{ where } \mathbf{n} = \mathbf{n}_0 \oplus \mathbf{n}_1 \\ \top & \text{otherwise} \end{cases}$$

We lift the above operation configuration-wise, and in this way obtain a new operation  $\hat{\oplus}$  on tuples of  $Const$  values.

*Example 1.* Consider the  $\overline{\text{IMP}}$  program  $S_1$ :

```

 $\mathbf{x} := 0;$ 
 $\# \text{if } (A) \mathbf{x} := \mathbf{x} + 1;$ 
 $\# \text{if } (B) \mathbf{x} := 1$ 
```

with the set  $\mathbb{K}_\psi = \{A \wedge B, A \wedge \neg B, \neg A \wedge B\}$ . By using the rules of Fig. 2, we can calculate  $\overline{\mathcal{A}}[S_1]$  for a store in which  $\mathbf{x}$  is uninitialized, i.e. it has the value  $\top$ . We assume a convention here that the first component of the store corresponds to configuration  $A \wedge B$ , the second to  $A \wedge \neg B$ , and the third to  $\neg A \wedge B$ . We write  $\overline{a_0} \xrightarrow{\overline{\mathcal{A}}[s]} \overline{a_1}$  when  $\overline{\mathcal{A}}[s]\overline{a_0} = \overline{a_1}$ . We have:

$$\begin{aligned} ([\mathbf{x} \mapsto \top], [\mathbf{x} \mapsto \top], [\mathbf{x} \mapsto \top]) &\xrightarrow{\overline{\mathcal{A}}[\mathbf{x}:=0]} ([\mathbf{x} \mapsto 0], [\mathbf{x} \mapsto 0], [\mathbf{x} \mapsto 0]) \\ &\xrightarrow{\overline{\mathcal{A}}[\# \text{if } (A) \mathbf{x}:=\mathbf{x}+1]} ([\mathbf{x} \mapsto 1], [\mathbf{x} \mapsto 1], [\mathbf{x} \mapsto 0]) \xrightarrow{\overline{\mathcal{A}}[\# \text{if } (B) \mathbf{x}:=1]} ([\mathbf{x} \mapsto 1], [\mathbf{x} \mapsto 1], [\mathbf{x} \mapsto 1]) \end{aligned}$$

After evaluating  $S_1$ , the variable  $\mathbf{x}$  has the constant value 1 for all valid configurations. Observe that in the above lifted stores many components are the same, i.e. many configurations have equivalent analysis information. Such lifted stores can be more compactly represented using sharing (e.g., bit vectors or formulae), which in effect will result in more efficient implementation of the lifted analysis.

Let  $S_2$  be a program obtained from  $S_1$ , such that  $\# \text{if } (B) \mathbf{x} := 1$  is replaced with  $\# \text{if } (B) \mathbf{x} := \mathbf{x} - 1$ . Then, we have:

$$\overline{\mathcal{A}}[S_2]([\mathbf{x} \mapsto \top], [\mathbf{x} \mapsto \top], [\mathbf{x} \mapsto \top]) = ([\mathbf{x} \mapsto 0], [\mathbf{x} \mapsto 1], [\mathbf{x} \mapsto -1])$$

We will use programs  $S_1$  and  $S_2$  as running examples throughout the paper.  $\square$

### 3 Variability Abstractions

When the set of configurations  $\mathbb{K}_\psi$  is large, calculations on the property domain  $\mathbb{A}^{\mathbb{K}_\psi}$  become expensive, even if using symbolic representations or sharing to avoid direct storage of  $|\mathbb{K}_\psi|$ -sized tuples as done in [5]. We want to replace  $\mathbb{A}^{\mathbb{K}_\psi}$  with a smaller domain obtained by abstraction and perform an approximate, but feasible, lifted analysis.



### 3.1 Basic Abstractions

We describe a compositional way of constructing abstractions over the domain  $\mathbb{A}^{\mathbb{K}}$ , where  $\mathbb{K}$  represents an arbitrary set of valid configurations, using two basic constructors, join and projection, along with a sequential and parallel composition of abstractions. The set of abstractions  $Abs$  is generated by the following grammar:

$$\alpha ::= \alpha^{\text{join}} \mid \alpha_{\varphi}^{\text{proj}} \mid \alpha \circ \alpha \mid \alpha \otimes \alpha \quad (1)$$

where  $\varphi \in \text{FeatExp}$ . Below we define the constructors and motivate them with examples. For readability, we use the constant propagation lattice  $\mathbb{A}$  however the results hold for any complete lattice.

*Join.* Consider the following scenario. An analysis is run interactively, while a developer is typing in a development environment. The analysis finds simple errors and warnings. In this scenario, the analysis must be fast and it should consider all legal configurations  $\mathbb{K}$ . It is not problematic if some spurious errors are introduced, since, like previously, a more thorough analysis is run regularly. Here, the precision with respect to configurations can be reduced by confounding the control-flow of all the products, obtaining an analysis that runs as if it was analyzing a single product, but involving code variants that participate in all products.

The *join* abstraction gathers the information about all valid configurations  $k \in \mathbb{K}$  into one value of  $\mathbb{A}$ . We formulate the abstraction  $\alpha^{\text{join}} : \mathbb{A}^{\mathbb{K}} \rightarrow \mathbb{A}^{\{\bigvee_{k \in \mathbb{K}} k\}}$  and the concretization function  $\gamma^{\text{join}} : \mathbb{A}^{\{\bigvee_{k \in \mathbb{K}} k\}} \rightarrow \mathbb{A}^{\mathbb{K}}$  as follows:

$$\alpha^{\text{join}}(\bar{a}) = (\bigsqcup_{k \in \mathbb{K}} \pi_k(\bar{a})) \quad \text{and} \quad \gamma^{\text{join}}(a) = \prod_{k \in \mathbb{K}} a \quad (2)$$

We overload abstraction names ( $\alpha$ ) to apply not only to domain elements but also to sets of features, sets of configurations, and, later, to program code. The new set of valid configurations is  $\alpha^{\text{join}}(\mathbb{K}) = \{\bigvee_{k \in \mathbb{K}} k\}$ . Thus, we have only one valid configuration denoted by the formula  $\bigvee_{k \in \mathbb{K}} k$ . Observe that this means that the obtained abstract domain is effectively  $\mathbb{A}^1$ , which is isomorphic to  $\mathbb{A}$ . The proposed abstraction–concretization pair is a Galois connection, which means that it can be used to construct analyses using calculational abstract interpretation:

**Theorem 1.**  $\langle \mathbb{A}^{\mathbb{K}}, \sqsubseteq \rangle \xleftrightarrow[\alpha^{\text{join}}]{\gamma^{\text{join}}} \langle \mathbb{A}^{\alpha^{\text{join}}(\mathbb{K})}, \sqsubseteq \rangle$  is a Galois connection <sup>3 4</sup>.

*Example 2.* Let us return to the scenario of using *join* for improving analysis performance. Assume that the feature model is given by  $\psi = A \vee B$  with valid configurations  $\mathbb{K}_{\psi} = \{A \wedge B, A \wedge \neg B, \neg A \wedge B\}$ . Now, the final stores we obtain by

<sup>3</sup>  $\langle L, \leq_L \rangle \xleftrightarrow[\alpha]{\gamma} \langle M, \leq_M \rangle$  is a Galois connection between complete lattices  $L$  and  $M$  iff  $\alpha$  and  $\gamma$  are total functions that satisfy:  $\alpha(l) \leq_M m \iff l \leq_L \gamma(m)$  for all  $l \in L, m \in M$ .

<sup>4</sup> The proofs of all theorems in this section can be found in App. A.

analyzing programs  $S_1$  and  $S_2$  from Example 1 are  $\bar{a}_{S_1} = ([x \mapsto 1], [x \mapsto 1], [x \mapsto 1])$  and  $\bar{a}_{S_2} = ([x \mapsto 0], [x \mapsto 1], [x \mapsto -1])$ . Applying the join abstraction we obtain  $\alpha^{\text{join}}(\bar{a}_{S_1}) = ([x \mapsto 1])$  and  $\alpha^{\text{join}}(\bar{a}_{S_2}) = ([x \mapsto \top])$ . In both cases the state representation has been significantly decreased. In the former case, the abstraction promptly notices that  $x$  is a constant regardless of the configuration. In the latter case, the abstraction loses precision by saying that  $x$  is not a constant in general, even if it was a constant in each of the configurations considered. We will continue using stores  $\bar{a}_{S_1}$  and  $\bar{a}_{S_2}$  in the subsequent examples.  $\square$

*Projection.* In industrial practice the number of products actually deployed is often only a small subset of  $\mathbb{K}$  [3]. In such case, analyzing all legal (valid) configurations seems unnecessary, and performance of analyses can be improved by abstracting many products away. This is achieved by a configuration projection, which removes configurations that do not satisfy a given constraint, for instance a disjunction of product configurations of interest. Projection can be helpful in other similar scenarios; for instance, to parallelize the analysis—by partitioning the product space using project and analyzing each partition separately.

Let  $\varphi$  be a formula over feature names. We define a *projection* abstraction mapping  $\mathbb{A}^{\mathbb{K}}$  into the domain  $\mathbb{A}^{\{k \in \mathbb{K} \mid k \models \varphi\}}$ , which preserves only the values corresponding to configurations from  $\mathbb{K}$  that satisfy  $\varphi$ . The information about configurations violating  $\varphi$  is disregarded. The abstraction and concretization functions between  $\mathbb{A}^{\mathbb{K}}$  and  $\mathbb{A}^{\{k \in \mathbb{K} \mid k \models \varphi\}}$  are defined as follows:

$$\alpha_{\varphi}^{\text{proj}}(\bar{a}) = \prod_{k \in \mathbb{K}, k \models \varphi} \pi_k(\bar{a}) \quad (3)$$

$$\gamma_{\varphi}^{\text{proj}}(\bar{a}') = \prod_{k \in \mathbb{K}} \begin{cases} \pi_k(\bar{a}') & \text{if } k \models \varphi \\ \top & \text{if } k \not\models \varphi \end{cases} \quad (4)$$

The new set of configurations is  $\alpha_{\varphi}^{\text{proj}}(\mathbb{K}) = \{k \in \mathbb{K} \mid k \models \varphi\}$ . Naturally, we also have a Galois connection here:

**Theorem 2.**  $\langle \mathbb{A}^{\mathbb{K}}, \sqsubseteq \rangle \xleftrightarrow[\alpha_{\varphi}^{\text{proj}}]{\gamma_{\varphi}^{\text{proj}}} \langle \mathbb{A}^{\alpha_{\varphi}^{\text{proj}}(\mathbb{K})}, \sqsubseteq \rangle$  is a Galois connection.

Notice that  $\alpha_{\text{true}}^{\text{proj}}$  is the identity function, since  $k \models \text{true}$  for all  $k \in \mathbb{K}$ . On the other hand  $\alpha_{\text{false}}^{\text{proj}}$  is the coarsest collapsing abstraction that maps any tuple into an empty one, since  $k \not\models \text{false}$ , for all  $k$ .

*Example 3.* Let us revisit our scenario, where a set of deployed configurations is much smaller than the set of configurations defined by the feature model  $\psi$ . Let us consider the store  $\bar{a}_{S_2}$  with the set of valid configurations  $\mathbb{K}_{\psi}$  from Example 2. The set of deployed products is defined by formula  $\varphi = A$  (so all possible programs with feature  $A$  are marketed). By definition of projection (3), we have:  $\alpha_A^{\text{proj}}(\bar{a}_{S_2}) = (\pi_{A \wedge B}(\bar{a}_{S_2}), \pi_{A \wedge \neg B}(\bar{a}_{S_2})) = ([x \mapsto 0], [x \mapsto 1])$ , and  $\alpha_{\neg A}^{\text{proj}}(\bar{a}_{S_2}) = (\pi_{\neg A \wedge B}(\bar{a}_{S_2})) = ([x \mapsto -1])$ . The state representation is effectively decreased to two, respectively one, components.  $\square$

An attentive reader, might discount the idea of the projection abstraction as being overly heavy. In the end, it appears to be equivalent to running the original analysis, just with a strengthened feature model  $(\psi \wedge \varphi)$ . However, as we shall see in the subsequent developments, projection is indeed useful. Thanks to the composition operators it can enter intricate scenarios, which cannot be expressed using a simple strengthening of a global feature model.

*Sequential Composition.* We use composition to build complex abstractions out of the basic ones, which also allows us to keep the number of operators in the framework and in the implementation low.

Recall that a composition of two Galois connections is also a Galois connection [9]. Let  $\langle \mathbb{A}^{\mathbb{K}}, \dot{\subseteq} \rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle \mathbb{A}^{\alpha_1(\mathbb{K})}, \dot{\subseteq} \rangle$  and  $\langle \mathbb{A}^{\alpha_1(\mathbb{K})}, \dot{\subseteq} \rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle \mathbb{A}^{\alpha_2(\alpha_1(\mathbb{K}))}, \dot{\subseteq} \rangle$  be two Galois connections. Then, we define their *composition* as  $\langle \mathbb{A}^{\mathbb{K}}, \dot{\subseteq} \rangle \xleftrightarrow[\alpha_2 \circ \alpha_1]{\gamma_1 \circ \gamma_2} \langle \mathbb{A}^{(\alpha_2 \circ \alpha_1)(\mathbb{K})}, \dot{\subseteq} \rangle$ , where

$$(\alpha_2 \circ \alpha_1)(\bar{a}) = \alpha_2(\alpha_1(\bar{a})) \quad \text{and} \quad (\gamma_1 \circ \gamma_2)(\bar{a}') = \gamma_1(\gamma_2(\bar{a}')) \quad (5)$$

for  $\bar{a} \in \mathbb{A}^{\mathbb{K}}$  and  $\bar{a}' \in \mathbb{A}^{(\alpha_2 \circ \alpha_1)(\mathbb{K})}$ . Also  $(\alpha_2 \circ \alpha_1)(\mathbb{K}) = \alpha_2(\alpha_1(\mathbb{K}))$ .

*Example 4.* Now consider the process of deriving an analysis, which only considers products actually deployed described by a formula  $\varphi$  (see previous example), but which should trade precision for speed, by confounding their execution. Such an analysis is derived using the composed abstraction:  $\alpha^{\text{join}} \circ \alpha_{\varphi}^{\text{proj}}$ .

Let  $\varphi = A$ . Configurations  $A \wedge B$  and  $A \wedge \neg B$  satisfy  $\varphi$ , whereas  $\neg \varphi$  is satisfied only by  $\neg A \wedge B$ . We have:  $\alpha^{\text{join}} \circ \alpha_A^{\text{proj}}(\bar{a}_{S_2}) = (\pi_{A \wedge B}(\bar{a}_{S_2}) \sqcup \pi_{A \wedge \neg B}(\bar{a}_{S_2})) = ([x \mapsto \top])$  and  $\alpha^{\text{join}} \circ \alpha_{\neg A}^{\text{proj}}(\bar{a}_{S_2}) = (\pi_{\neg A \wedge B}(\bar{a}_{S_2})) = ([x \mapsto \neg 1])$ .  $\square$

*Parallel Composition.* Consider a product line where two disjoint groups of products share the same code base: one group is correctness critical, the other comprises correctness non-critical products. The former should be analyzed with highest precision possible to obtain the most precise analysis results, the latter can be analyzed faster. We can set up such analyses by using a projection abstraction to analyze the correctness critical group precisely, and the join abstraction to analyze the non-critical group. However running the analyses twice, ignores the fact that the code is shared between the groups. We can combine two separate analyses by creating a compound abstraction: a *product* of the two. The product abstraction will correspond exactly to executing the projection on the correctness critical products, and join on the non-critical ones. But since the product creates a single Galois connection of the two, it can be used to derive an analysis which will deliver this in a single run, which is more efficient overall, due to reuse of the states explored.

Galois connections  $\langle \mathbb{A}^{\mathbb{K}}, \dot{\subseteq} \rangle \xleftrightarrow[\alpha_1]{\gamma_1} \langle \mathbb{A}^{\alpha_1(\mathbb{K})}, \dot{\subseteq} \rangle$  and  $\langle \mathbb{A}^{\mathbb{K}}, \dot{\subseteq} \rangle \xleftrightarrow[\alpha_2]{\gamma_2} \langle \mathbb{A}^{\alpha_2(\mathbb{K})}, \dot{\subseteq} \rangle$  over the same domain  $\mathbb{A}^{\mathbb{K}}$  can be composed into one that combines the abstraction results "side-by-side". The result is a new compound abstraction,  $\alpha_1 \otimes \alpha_2$ , of the domain  $\mathbb{A}^{\mathbb{K}}$  obtained by applying the two simpler abstractions in parallel. The parallel composition of abstractions is defined using a direct tensor product. For

the resulting Galois connection, we have  $\alpha_1 \otimes \alpha_2(\mathbb{K}) = \alpha_1(\mathbb{K}) \cup \alpha_2(\mathbb{K})$ . Given  $\bar{a}_1 \in \mathbb{A}^{\alpha_1(\mathbb{K})}$  and  $\bar{a}_2 \in \mathbb{A}^{\alpha_2(\mathbb{K})}$ , we first define  $\bar{a}_1 \times \bar{a}_2 \in \alpha_1(\mathbb{K}) \cup \alpha_2(\mathbb{K})$  as:

$$\bar{a}_1 \times \bar{a}_2 = \prod_{k \in \alpha_1(\mathbb{K}) \cup \alpha_2(\mathbb{K})} \begin{cases} \pi_k(\bar{a}_1) & \text{if } k \in \alpha_1(\mathbb{K}) \setminus \alpha_2(\mathbb{K}) \\ \pi_k(\bar{a}_1) \sqcup \pi_k(\bar{a}_2) & \text{if } k \in \alpha_1(\mathbb{K}) \cap \alpha_2(\mathbb{K}) \\ \pi_k(\bar{a}_2) & \text{if } k \in \alpha_2(\mathbb{K}) \setminus \alpha_1(\mathbb{K}) \end{cases} \quad (6)$$

The direct tensor product is given as  $\langle \mathbb{A}^{\mathbb{K}}, \dot{\sqsubseteq} \rangle \xleftrightarrow[\alpha_1 \otimes \alpha_2]{\gamma_1 \otimes \gamma_2} \langle \mathbb{A}^{(\alpha_1 \otimes \alpha_2)(\mathbb{K})}, \dot{\sqsubseteq} \rangle$ , where

$$(\alpha_1 \otimes \alpha_2)(\bar{a}) = \alpha_1(\bar{a}) \times \alpha_2(\bar{a}) \quad (7)$$

$$(\gamma_1 \otimes \gamma_2)(\bar{a}') = \gamma_1(\pi_{\alpha_1(\mathbb{K})}(\bar{a}')) \sqcap \gamma_2(\pi_{\alpha_2(\mathbb{K})}(\bar{a}')) \text{ , where} \quad (8)$$

$\pi_{\alpha_1(\mathbb{K})}(\bar{a}') = \prod_{k \in \alpha_1(\mathbb{K})} \pi_k(\bar{a}')$  and  $\pi_{\alpha_2(\mathbb{K})}(\bar{a}') = \prod_{k \in \alpha_2(\mathbb{K})} \pi_k(\bar{a}')$ , for  $\bar{a}' \in \mathbb{A}^{(\alpha_1 \otimes \alpha_2)(\mathbb{K})}$ .

**Theorem 3.**  $\langle \mathbb{A}^{\mathbb{K}}, \dot{\sqsubseteq} \rangle \xleftrightarrow[\alpha_1 \otimes \alpha_2]{\gamma_1 \otimes \gamma_2} \langle \mathbb{A}^{(\alpha_1 \otimes \alpha_2)(\mathbb{K})}, \dot{\sqsubseteq} \rangle$  is a Galois connection.

*Example 5.* Let us assume that for products with feature  $A$  we need precise analysis results, and for products without this feature we do not need so precise results. We are interested in analyzing products with  $A$  thoroughly, while the analysis of the products without  $A$  can be speeded up. To this end we build the following abstraction:  $\alpha_A^{\text{proj}} \otimes (\alpha^{\text{join}} \circ \alpha_{\neg A}^{\text{proj}})$ .  $\square$

### 3.2 Derived Abstractions

We shall now discuss three more abstractions that can be derived from the above basic constructors.

*Join-Project.* Recall the construction of Example 4, where we combined projection with a join in order to confound a subset of legal configurations. This pattern has occurred so often in our exercises that we introduced a syntactic sugar for it. For a formula  $\varphi$  over features, the abstraction  $\alpha_\varphi^{\text{join}}$  gathers the information about all valid configurations  $k \in \mathbb{K}$  that satisfy  $\varphi$ , i.e.  $k \models \varphi$ , into one value of  $\mathbb{A}$ , whereas the information about all other valid configurations  $k \in \mathbb{K}$  that do not satisfy  $\varphi$  is disregarded. We define

$$\alpha_\varphi^{\text{join}} = \alpha^{\text{join}} \circ \alpha_\varphi^{\text{proj}} \quad \text{and} \quad \gamma_\varphi^{\text{join}} = \gamma_\varphi^{\text{proj}} \circ \gamma^{\text{join}} \quad (9)$$

where we have that  $\langle \mathbb{A}^{\mathbb{K}}, \dot{\sqsubseteq} \rangle \xleftrightarrow[\alpha_\varphi^{\text{proj}}]{\gamma_\varphi^{\text{proj}}} \langle \mathbb{A}^{\alpha_\varphi^{\text{proj}}(\mathbb{K})}, \dot{\sqsubseteq} \rangle$  and  $\langle \mathbb{A}^{\alpha_\varphi^{\text{proj}}(\mathbb{K})}, \dot{\sqsubseteq} \rangle \xleftrightarrow[\alpha^{\text{join}}]{\gamma^{\text{join}}} \langle \mathbb{A}^{(\alpha^{\text{join}} \circ \alpha_\varphi^{\text{proj}})(\mathbb{K})}, \dot{\sqsubseteq} \rangle$  are Galois connections. Now the compositions in Example 4 can be written simply as  $\alpha_A^{\text{join}}$  and  $\alpha_{\neg A}^{\text{join}}$ .

*Ignoring features.* Consider a scenario, where a configurable third-party component is integrated into a product line. The code base is large, and a static analysis does not scale to this size. In a compile-analyze-test cycle errors appear most often in the newly written code, and are thus relatively little influenced by how the features of the third party component are configured. Lowering precision on analyzing external components can allow finding errors faster. This scenario can be realized using a feature projection, which simplifies feature domains by confounding executions differing only on uninteresting features.

Before defining feature projection, let us consider a simpler case of ignoring a single feature  $A \in \mathbb{F}$  that is not directly relevant for current analysis. The *ignore feature* abstraction merges any configurations that only differ with regard to  $A$ , and are identical with regard to remaining features,  $\mathbb{F} \setminus \{A\}$ . We write  $\varphi \setminus A$  for a formula obtained by eliminating variable  $A$  from  $\varphi$ . The actual method of variable elimination is insignificant, as we assume all equivalent formulas as identical in this paper. The new set of configurations is given by  $\alpha_A^{\text{ignore}}(\mathbb{K}) = \{\bigvee_{k \in \mathbb{K}, k \setminus A \equiv k'} k \mid k' \in \{k \setminus A \mid k \in \mathbb{K}\}\}$ . The abstraction  $\alpha_A^{\text{ignore}} : \mathbb{A}^{\mathbb{K}} \rightarrow \mathbb{A}^{\alpha_A^{\text{ignore}}(\mathbb{K})}$  and concretization functions  $\gamma_A^{\text{ignore}} : \mathbb{A}^{\alpha_A^{\text{ignore}}(\mathbb{K})} \rightarrow \mathbb{A}^{\mathbb{K}}$  are:

$$\alpha_A^{\text{ignore}}(\bar{a}) = \prod_{k' \in \alpha_A^{\text{ignore}}(\mathbb{K})} \bigsqcup_{k \in \mathbb{K}, k \models k'} \pi_k(\bar{a}) \quad (10)$$

$$\gamma_A^{\text{ignore}}(\bar{a}') = \prod_{k \in \mathbb{K}} \pi_{k'}(\bar{a}') \text{ if } k \models k' \quad (11)$$

It turns out that ignoring features can be derived from the above basic abstractions as shown in the following theorem:

**Theorem 4.** *Let  $\alpha_A^{\text{ignore}}(\mathbb{K}) = \{k'_1, \dots, k'_n\}$ . Then:*

$$\alpha_A^{\text{ignore}} = \alpha_{k'_1}^{\text{join}} \otimes \dots \otimes \alpha_{k'_n}^{\text{join}} \quad \text{and} \quad \gamma_A^{\text{ignore}} = \gamma_{k'_1}^{\text{join}} \otimes \dots \otimes \gamma_{k'_n}^{\text{join}}.$$

*Example 6.* We consider the lifted store  $\bar{a}_{S_2}$  with  $\mathbb{K}_\psi = \{A \wedge B, A \wedge \neg B, \neg A \wedge B\}$ . Then, we have  $\alpha_A^{\text{ignore}}(\mathbb{K}_\psi) = \{(A \wedge B) \vee (\neg A \wedge B), A \wedge \neg B\}$  and  $\alpha_A^{\text{ignore}}(\bar{a}_{S_2}) = (\pi_{A \wedge B}(\bar{a}_{S_2}) \sqcup \pi_{\neg A \wedge B}(\bar{a}_{S_2}), \pi_{A \wedge \neg B}(\bar{a}_{S_2})) = ([x \mapsto \top], [x \mapsto 1])$ . On the other hand, we have  $\alpha_B^{\text{ignore}}(\mathbb{K}_\psi) = \{(A \wedge B) \vee (A \wedge \neg B), \neg A \wedge B\}$  and  $\alpha_B^{\text{ignore}}(\bar{a}_{S_2}) = (\pi_{A \wedge B}(\bar{a}_{S_2}) \sqcup \pi_{A \wedge \neg B}(\bar{a}_{S_2}), \pi_{\neg A \wedge B}(\bar{a}_{S_2})) = ([x \mapsto \top], [x \mapsto -1])$ .  $\square$

*Feature Projection.* Now, if we need to ignore a larger number of features (say features outside a certain component of interest), we can do it using a feature projection operator which simply ignores a set of features  $\{A_1, \dots, A_k\} \subseteq \mathbb{F}$ :

$$\alpha_{\{A_1, \dots, A_k\}}^{\text{fproj}} = \alpha_{A_1}^{\text{ignore}} \circ \dots \circ \alpha_{A_k}^{\text{ignore}} \quad \text{and} \quad \gamma_{\{A_1, \dots, A_k\}}^{\text{fproj}} = \gamma_{A_k}^{\text{ignore}} \circ \dots \circ \gamma_{A_1}^{\text{ignore}}$$

It follows from the theorems of Section 3.1 that all the derived pairs of abstraction-concretization are Galois connections.

## 4 Abstracting Lifted Analyses

We will now demonstrate how to derive abstracted lifted analyses using the operators of Section 3, using the case of constant propagation for IMP programs

$$\begin{aligned}
& (\alpha \circ \overline{\mathcal{A}}[\text{\#if } (\theta) s] \circ \gamma)(\bar{d}) = \alpha(\overline{\mathcal{A}}[\text{\#if } (\theta) s](\gamma(\bar{d}))) = & \text{(by def. of } \circ) \\
& = \alpha \left( \prod_{k \in \mathbb{K}_\psi} \begin{cases} \pi_k(\overline{\mathcal{A}}[s]\gamma(\bar{d})) & \text{if } k \models \theta \\ \pi_k(\gamma(\bar{d})) & \text{if } k \not\models \theta \end{cases} \right) & \text{(def. of } \overline{\mathcal{A}} \text{ in Fig. 2)} \\
& \sqsubseteq \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\alpha(\overline{\mathcal{A}}[s]\gamma(\bar{d}))) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha(\gamma(\bar{d}))) \sqcup \pi_{k'}(\alpha(\overline{\mathcal{A}}[s]\gamma(\bar{d}))) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\alpha(\gamma(\bar{d}))) & \text{if } k' \models \neg \theta \end{cases} & \text{(Lemma 2, App. C)} \\
& \sqsubseteq \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_\alpha[s]\bar{d}) & \text{if } k' \models \theta \\ \pi_{k'}(\bar{d}) \sqcup \pi_{k'}(\overline{\mathcal{D}}_\alpha[s]\bar{d}) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\bar{d}) & \text{if } k' \models \neg \theta \end{cases} & \text{(by IH and } \alpha \circ \gamma \text{ reductive)} \\
& = \overline{\mathcal{D}}_\alpha[\text{\#if } (\theta) s] \bar{d}
\end{aligned}$$

**Fig. 3.** Calculational derivation of  $\overline{\mathcal{D}}_\alpha[\text{\#if } (\theta) s]$ , the abstraction of  $\overline{\mathcal{A}}[\text{\#if } (\theta) s]$ . The ‘reductive’ property of all Galois connections is  $(\alpha \circ \gamma)(\bar{d}) \sqsubseteq \bar{d}$  for all  $\bar{d}$ .

as an example. Recall that this analysis has been specified by: 1) the domain  $\mathbb{A}^{\mathbb{K}_\psi}$ ; 2) the statement transfer function  $\overline{\mathcal{A}}[s] : (\mathbb{A} \rightarrow \mathbb{A})^{\mathbb{K}_\psi}$ ; and 3) the expression evaluation function  $\overline{\mathcal{A}}'[e] : (\mathbb{A} \rightarrow \text{Const})^{\mathbb{K}_\psi}$ . Let  $\langle \mathbb{A}^{\mathbb{K}_\psi}, \sqsubseteq \rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathbb{A}^{\alpha(\mathbb{K}_\psi)}, \sqsubseteq \rangle$  be a Galois connection constructed using the abstractions presented in Section 3. We will also write  $(\alpha, \gamma) \in \text{Abs}$  to denote a Galois connection obtained in such way.

Any function  $f$  defined on the concrete domain of a Galois connection can be abstracted to work on the abstract domain by applying concretization to its argument and an abstraction to its value, i.e. by the function  $F = \alpha \circ f \circ \gamma$ , where  $\circ$  denotes the usual composition of functions. In fact, any monotone over-approximation of the composition  $\alpha \circ f \circ \gamma$  is sufficient for a sound analysis. Even fixed points can be transferred from a concrete to an abstract domain of a Galois connection. If both domains are complete lattices and  $f$  is a monotone function on the concrete domain, then by the fixed point transfer theorem (FPT for short) [8]:  $\alpha(\text{lfp} f) \sqsubseteq \text{lfp} F \sqsubseteq \text{lfp} F^\#$ . Here  $F = \alpha \circ f \circ \gamma$  and  $F^\#$  is some monotone, conservative *over*-approximation of  $F$ , i.e.  $F \sqsubseteq F^\#$ . The calculational approach to abstract interpretation [11] used in this work, advocates simple algebraic manipulation to obtain a *direct expression* for the function  $F$  (if it exists) or for an over-approximation  $F^\#$ .

In our case, for any lifted store  $\bar{a} \in \mathbb{A}^{\mathbb{K}_\psi}$ , we calculate an abstracted lifted store by  $\alpha(\bar{a}) = \bar{d} \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)}$ . Now, we use a Galois connection to derive an over-approximation of  $\alpha \circ \overline{\mathcal{A}}[s] \circ \gamma$  obtaining a new abstracted statement transfer function  $\overline{\mathcal{D}}_\alpha[s] : (\mathbb{A} \rightarrow \mathbb{A})^{\alpha(\mathbb{K}_\psi)}$ . Similarly, one can derive an abstracted analysis for expressions  $\overline{\mathcal{D}}'_\alpha[e]$ , approximating  $\alpha \circ \overline{\mathcal{A}}'[e] \circ \gamma$ . These approximations are derived using structural induction on statements (respectively on expressions),

$$\begin{aligned}
& (\alpha \circ \overline{\mathcal{A}'}[e_0 \oplus e_1] \circ \gamma)(\bar{d}) \\
&= \alpha \left( \prod_{k \in \mathbb{K}_\psi} \pi_k(\overline{\mathcal{A}'}[e_0]\gamma(\bar{d})) \hat{\oplus} \pi_k(\overline{\mathcal{A}'}[e_1]\gamma(\bar{d})) \right) \quad (\text{by def. of } \circ, \text{ and } \overline{\mathcal{A}'} \text{ in Fig. 2}) \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\alpha(\overline{\mathcal{A}'}[e_0]\gamma(\bar{d})) \hat{\oplus} \alpha(\overline{\mathcal{A}'}[e_1]\gamma(\bar{d}))) \quad (\text{by def. of } \pi_k, \hat{\oplus}, \text{ and } \alpha) \\
&\dot{\subseteq} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\alpha(\overline{\mathcal{A}'}[e_0]\gamma(\bar{d})) \hat{\oplus} \alpha(\overline{\mathcal{A}'}[e_1]\gamma(\bar{d}))) \quad (\text{by Lemma 3 in App. C}) \\
&\dot{\subseteq} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\overline{\mathcal{D}'}_\alpha[e_0]\bar{d}) \hat{\oplus} \pi_{k'}(\overline{\mathcal{D}'}_\alpha[e_1]\bar{d}) \quad (\text{by IH, and def. of } \pi_{k'} \text{ and } \hat{\oplus}) \\
&= \overline{\mathcal{D}'}_\alpha[e_0 \oplus e_1]\bar{d}
\end{aligned}$$

**Fig. 4.** Calculational derivation of  $\overline{\mathcal{D}}_\alpha[e_0 \oplus e_1]$ .

in a process that resembles a simple algebraic calculation, deceptively akin to equation reasoning.

Let us consider the derivation steps for the static conditional statement (**#if** ( $\theta$ )  $s$ ) in detail. Our inductive hypothesis (IH) is that for statements  $s'$  that are structurally smaller than (**#if** ( $\theta$ )  $s$ ) the (yet-to-be-calculated)  $\overline{\mathcal{D}}_\alpha[s']$  soundly approximates  $\alpha \circ \overline{\mathcal{A}}[s'] \circ \gamma$ , formally:  $\alpha \circ \overline{\mathcal{A}}[s'] \circ \gamma \dot{\subseteq} \overline{\mathcal{D}}_\alpha[s']$ . The derivation in Fig. 3 begins with composing the concretization and abstraction functions with the concrete transfer function and then proceeds by expanding definitions. An (inner) induction on the structure of the abstraction  $\alpha$  follows, delegated to the Appendix for brevity. In the last step we apply the inductive hypothesis, to obtain a closed representation independent of  $\overline{\mathcal{A}}$ . This representation, just before the final equality, is the newly obtained (calculated) definition of the abstracted analysis  $\overline{\mathcal{D}}_\alpha$ . Interestingly, the derivation is independent of the structure of the abstraction  $\alpha$ , so this form works for any abstraction specified using our operators. We give a sketch of derivational steps for  $e_0 \oplus e_1$  in Fig. 4.

The derivations for other cases are similar and can be found in App. B. The process results in the definitions of  $\overline{\mathcal{D}}_\alpha[s]$  and  $\overline{\mathcal{D}'}_\alpha[e]$  presented in Fig. 5. Monotonicity of  $\overline{\mathcal{D}}_\alpha[s]$  and  $\overline{\mathcal{D}'}_\alpha[e]$  is shown in App. D. Soundness of the abstracted analysis follows by construction; more precisely the complete calculation constitutes an inductive proof of the following theorem:

**Theorem 5 (Soundness of Abstracted Analysis).**

- (i)  $\forall e \in \text{Exp}, (\alpha, \gamma) \in \text{Abs}, \bar{d} \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)} : \alpha \circ \overline{\mathcal{A}'}[e] \circ \gamma(\bar{d}) \dot{\subseteq} \overline{\mathcal{D}'}_\alpha[e] \bar{d}$
- (ii)  $\forall s \in \text{Stm}, (\alpha, \gamma) \in \text{Abs}, \bar{d} \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)} : \alpha \circ \overline{\mathcal{A}}[s] \circ \gamma(\bar{d}) \dot{\subseteq} \overline{\mathcal{D}}_\alpha[s] \bar{d}$

*Example 7.* Consider the program  $S_1$  from Example 1, with  $\mathbb{K}_\psi = \{A \wedge B, A \wedge \neg B, \neg A \wedge B\}$ . We calculate  $\overline{\mathcal{D}}_{\alpha_1}[S_1]$  for  $\alpha_1 = \alpha_A^{\text{join}}$ . Following the rules of Fig. 5, we obtain the following confounded abstract execution off all configurations

$$\begin{aligned}
\overline{\mathcal{D}}_\alpha[\text{skip}] &= \lambda \bar{d}. \bar{d} \\
\overline{\mathcal{D}}_\alpha[\mathbf{x} := e] &= \lambda \bar{d}. \prod_{k' \in \alpha(\mathbb{K}_\psi)} (\pi_{k'}(\bar{d}))[\mathbf{x} \mapsto \pi_{k'}(\overline{\mathcal{D}}'_\alpha[e]\bar{d})] \\
\overline{\mathcal{D}}_\alpha[s_0 ; s_1] &= \overline{\mathcal{D}}_\alpha[s_1] \circ \overline{\mathcal{D}}_\alpha[s_0] \\
\overline{\mathcal{D}}_\alpha[\text{if } e \text{ then } s_0 \text{ else } s_1] &= \lambda \bar{d}. \overline{\mathcal{D}}_\alpha[s_0]\bar{d} \dot{\cup} \overline{\mathcal{D}}_\alpha[s_1]\bar{d} \\
\overline{\mathcal{D}}_\alpha[\text{while } e \text{ do } s] &= \text{lfp} \lambda \bar{\Phi}. \lambda \bar{d}. \bar{d} \dot{\cup} \bar{\Phi}(\overline{\mathcal{D}}_\alpha[s]\bar{d}) \\
\overline{\mathcal{D}}_\alpha[\text{\#if } (\theta) \ s] &= \lambda \bar{d}. \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_\alpha[s]\bar{d}) & \text{if } k' \models \theta \\ \pi_{k'}(\bar{d}) \dot{\cup} \pi_{k'}(\overline{\mathcal{D}}_\alpha[s]\bar{d}) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\bar{d}) & \text{if } k' \models \neg \theta \end{cases} \\
\overline{\mathcal{D}}'_\alpha[n] &= \lambda \bar{d}. \prod_{k' \in \alpha(\mathbb{K}_\psi)} n \\
\overline{\mathcal{D}}'_\alpha[\mathbf{x}] &= \lambda \bar{d}. \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\bar{d})(\mathbf{x}) \\
\overline{\mathcal{D}}'_\alpha[e_0 \oplus e_1] &= \lambda \bar{d}. \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\overline{\mathcal{D}}'_\alpha[e_0]\bar{d}) \hat{\oplus} \pi_{k'}(\overline{\mathcal{D}}'_\alpha[e_1]\bar{d})
\end{aligned}$$

**Fig. 5.** Definitions of  $\overline{\mathcal{D}}_\alpha[\bar{s}] : (\mathbb{A} \rightarrow \mathbb{A})^{\alpha(\mathbb{K}_\psi)}$  and  $\overline{\mathcal{D}}'_\alpha[\bar{e}] : (\mathbb{A} \rightarrow \text{Const})^{\alpha(\mathbb{K}_\psi)}$ .

containing the feature  $A$ :

$$([\mathbf{x} \mapsto \top]) \xrightarrow{\overline{\mathcal{D}}_{\alpha_1}[\mathbf{x} := 0]} ([\mathbf{x} \mapsto 0]) \xrightarrow{\overline{\mathcal{D}}_{\alpha_1}[\text{\#if } (A) \ \mathbf{x} := \mathbf{x} + 1]} ([\mathbf{x} \mapsto 1]) \xrightarrow{\overline{\mathcal{D}}_{\alpha_1}[\text{\#if } (B) \ \mathbf{x} := 1]} ([\mathbf{x} \mapsto 1])$$

In the last step we used  $\overline{\mathcal{D}}_{\alpha_1}[\text{\#if } (B) \ \mathbf{x} := 1]([\mathbf{x} \mapsto 1]) = ([\mathbf{x} \mapsto 1]) \dot{\cup} \overline{\mathcal{D}}_{\alpha_1}[\mathbf{x} := 1]([\mathbf{x} \mapsto 1])$  since  $((A \wedge B) \vee (A \wedge \neg B)) \wedge B$  and  $((A \wedge B) \vee (A \wedge \neg B)) \wedge \neg B$  are both satisfiable. The final result shows that the value of  $\mathbf{x}$  is the constant 1 for every configuration that satisfies  $A$ . On the other hand, for the program  $S_2$  and the same abstraction we obtain  $\overline{\mathcal{D}}_{\alpha_1}[S_2]([\mathbf{x} \mapsto \top]) = ([\mathbf{x} \mapsto \top])$ , so the value of  $x$  is lost (approximated) by  $\overline{\mathcal{D}}_{\alpha_1}$ .  $\square$

We may implement the abstracted analysis in Fig. 5 directly by using Kleene's fixed point theorem to calculate fixed points of loops iteratively. But, we can also extract corresponding data-flow equations, and then apply the known iterative algorithms to calculate fixed-point solutions. We assume that the individual statements are uniquely labelled with labels  $\ell$ . Given an abstraction  $\alpha$ , for each statement  $s^\ell$  we generate two abstracted stores  $\llbracket s^\ell \rrbracket_{\text{in}}^\alpha, \llbracket s^\ell \rrbracket_{\text{out}}^\alpha : \mathbb{A}^{\alpha(\mathbb{K}_\psi)}$ , which describe the input and output abstract store for all configurations before and after executing the statement  $s^\ell$ . They are related with the definitions for abstracted analysis  $\overline{\mathcal{D}}_\alpha$  given in Fig. 5 as follows: for each statement  $s$  the input store  $\llbracket s^\ell \rrbracket_{\text{in}}^\alpha$  is substituted for the parameter  $\bar{d}$ , and the output store  $\llbracket s^\ell \rrbracket_{\text{out}}^\alpha$  for the value of the corresponding function. Some variability dependent data-flow equations are



$$\begin{aligned}
& \forall k' \in \alpha(\mathbb{K}_\psi): \pi_{k'}(\llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{out}}^\alpha) = \pi_{k'}(\llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{in}}^\alpha) [x \mapsto \pi_{k'}(\overline{\mathcal{D}}'_\alpha \llbracket e^{\ell_0} \rrbracket [x :=^\ell e^{\ell_0}]_{\text{in}}^\alpha)] \\
& \forall k' \in \alpha(\mathbb{K}_\psi): \pi_{k'}(\llbracket \text{\#if}^\ell(\theta) s^{\ell_0} \rrbracket_{\text{out}}^\alpha) = \begin{cases} \pi_{k'}(\llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) & \text{if } k' \models \theta \\ \pi_{k'}(\llbracket \text{\#if}^\ell(\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \sqcup \pi_{k'}(\llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\llbracket \text{\#if}^\ell(\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) & \text{if } k' \models \neg \theta \end{cases} \\
& \forall k' \in \alpha(\mathbb{K}_\psi): \pi_{k'}(\llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha) = \pi_{k'}(\llbracket \text{\#if}^\ell(\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \quad \text{if } \text{sat}(k' \wedge \theta)
\end{aligned}$$

**Fig. 6.** Selected data-flow equations for abstracted constant propagation.

given in Fig 6. The complete list of data-flow equations along with the proof of their soundness can be found in App. E.

## 5 Variability Abstraction with Syntactic Transformation

The analyses  $\overline{\mathcal{A}}$  and  $\overline{\mathcal{D}}_\alpha$  can be implemented either directly by using definitions of Figs. 2 and 5, or by extracting the corresponding data-flow equations. An entirely different way to implement  $\overline{\mathcal{D}}_\alpha$  is to execute the abstraction on the source program, before running the analysis, and then running the previously existing analysis  $\overline{\mathcal{A}}$  on this transformed program. We take this route as it allows to completely reuse the effort invested in designing and implementing  $\overline{\mathcal{A}}$ .

Any  $\overline{\text{IMP}}$  program  $s$  with sets of features  $\mathbb{F}$  and valid configurations  $\mathbb{K}$  is translated into a corresponding abstract program  $\alpha(s)$  with corresponding set of features  $\alpha(\mathbb{F})$  and set of valid configurations  $\alpha(\mathbb{K})$ . We define the translation recursively over the structure of  $\alpha$ . All statements other than  $\text{\#if}$  are copied. For example,  $\alpha(\text{skip}) = \text{skip}$  and  $\alpha(s_0 ; s_1) = \alpha(s_0) ; \alpha(s_1)$ . We discuss the rewrites for  $\text{\#if}$  statements below.

In the rewrite, we associate a fresh feature name  $Z \notin \mathbb{F}$ , with every join abstraction  $\alpha_Z^{\text{join}}$  (consequently written  $\alpha_{Z'}^{\text{join}}$ ). The new feature  $Z$  is an abstract name (renaming) of the compound formula  $\bigvee_{k \in \mathbb{K}} k$ . It denotes the single valid configuration obtained from  $\alpha^{\text{join}}$ . The new feature name is used to simplify conditions in the transformed code. The  $\alpha_Z^{\text{join}}$  rewrite is defined as follows:

$$\begin{aligned}
& \alpha_Z^{\text{join}}(\mathbb{F}) = \{Z\}, \quad \alpha_Z^{\text{join}}(\mathbb{K}) = \{Z\} \\
& \alpha_Z^{\text{join}}(\text{\#if}(\theta) s) = \begin{cases} \text{\#if}(Z) \alpha_Z^{\text{join}}(s) & \text{if } \bigvee_{k \in \mathbb{K}} k \models \theta \\ \text{\#if}(Z) \text{lub}(\alpha_Z^{\text{join}}(s), \text{skip}) & \text{if } \text{sat}(\bigvee_{k \in \mathbb{K}} k \wedge \theta) \wedge \text{sat}(\bigvee_{k \in \mathbb{K}} k \wedge \neg \theta) \\ \text{\#if}(\neg Z) \alpha_Z^{\text{join}}(s) & \text{if } \bigvee_{k \in \mathbb{K}} k \models \neg \theta \end{cases}
\end{aligned}$$

In effect of applying the  $\alpha_Z^{\text{join}}$  transformation to any program  $s$  we obtain a single variant program, i.e. a SPL with only one valid product where the feature  $Z$  is enabled. It can be analyzed with existing single-program analyses.

Note that it enables performing family-based analyses with implementations of single-program analyses, albeit with loss of precision. The newly introduced statement  $\text{lub}(s_0, s_1)$  represents the least upper bound (join) of the results obtained by executing  $s_0$  and  $s_1$ . This is the only language-dependent aspect of **reconfigurator**. It can have different implementations depending on the programming language and the analysis we work with. In our case, we exploit the fact that  $\overline{A}[\text{if } e \text{ then } s_0 \text{ else } s_1]$  ignores the branching condition (cf. Fig. 2) and use  $\text{lub}(s_0, s_1) = \text{if } (n) \text{ then } s_0 \text{ else } s_1$  for some fixed integer  $n$ . Finally, observe that  $\# \text{if } (\neg Z) \alpha_Z^{\text{join}}(s)$  is equivalent to **skip**, however it is useful to keep the statement in the program, which makes it easy to merge programs when we use compound abstractions (below).

The rewrite for projection only changes the set of legal configurations:

$$\alpha_\varphi^{\text{proj}}(\mathbb{F}) = \mathbb{F}, \quad \alpha_\varphi^{\text{proj}}(\mathbb{K}) = \{k \in \mathbb{K} \mid k \models \varphi\}, \quad \alpha_\varphi^{\text{proj}}(\# \text{if } (\theta) s) = \# \text{if } (\theta) \alpha_\varphi^{\text{proj}}(s)$$

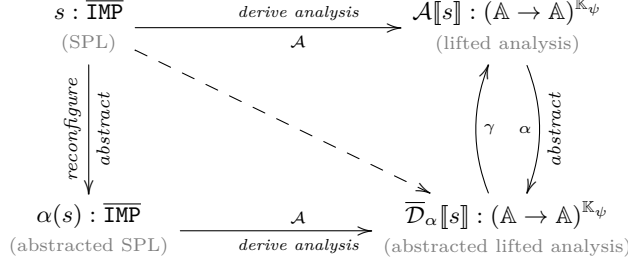
Note that the general scheme for the basic rewrites of **#if** statements can be summarized as  $\alpha(\# \text{if } (\theta) s) = \# \text{if } (\overline{\alpha}(\theta)) \overline{\alpha}(s, \theta)$ , where  $\overline{\alpha}$  are functions transforming the condition  $\theta$  and the statement  $s$ . It is easy to extract  $\overline{\alpha}(\theta)$  and  $\overline{\alpha}(s, \theta)$  from the above rewrites for  $\alpha_Z^{\text{join}}$  and  $\alpha_\varphi^{\text{proj}}$ . We will use them in defining transformations for binary operators.

Now, for the case of parallel composition  $\alpha_1 \otimes \alpha_2$ , recall that the set  $\alpha_1 \otimes \alpha_2(\mathbb{K})$  is the union of  $\alpha_1(\mathbb{K})$  and  $\alpha_2(\mathbb{K})$ . However in the rewrite semantics, we are sometimes modifying the set of features. If  $\alpha_1(\mathbb{F}) \neq \alpha_2(\mathbb{F})$  then some of valid configurations in  $\alpha_1(\mathbb{K}) \cup \alpha_2(\mathbb{K})$  will not assign truth values to all features in  $\alpha_1(\mathbb{F}) \cup \alpha_2(\mathbb{F})$ . To take a meaningful union of configurations, we need to first unify their alphabets. To achieve this aim, each valid configuration can be extended by information that the missing features are excluded from it (negated). Now the rewrite rules for parallel composition are given by:

$$\begin{aligned} \alpha_1 \otimes \alpha_2(\mathbb{F}) &= \alpha_1(\mathbb{F}) \cup \alpha_2(\mathbb{F}) \\ \alpha_1 \otimes \alpha_2(\mathbb{K}) &= \{k_1 \wedge \bigwedge_{f \in \alpha_2(\mathbb{F}) \setminus \alpha_1(\mathbb{F})} \neg f \mid k_1 \in \alpha_1(\mathbb{K})\} \cup \{k_2 \wedge \bigwedge_{f \in \alpha_1(\mathbb{F}) \setminus \alpha_2(\mathbb{F})} \neg f \mid k_2 \in \alpha_2(\mathbb{K})\} \\ \alpha_1 \otimes \alpha_2(\# \text{if } (\theta) s) &= \begin{cases} \# \text{if } (\overline{\alpha}_1(\theta) \vee \overline{\alpha}_2(\theta)) \overline{\alpha}_1(s, \theta) & \text{if } \overline{\alpha}_1(s, \theta) = \overline{\alpha}_2(s, \theta) \\ \alpha_1(\# \text{if } (\theta) s); \alpha_2(\# \text{if } (\theta) s) & \text{otherwise} \end{cases} \end{aligned}$$

Observe that the second case of the parallel composition transformation can only appear if the second case of a join transformation has been used somewhere in recursive rewriting of  $s$  (perhaps deep). All the other rewrites leave  $s$  intact. However, in such case the branches have disjoint feature alphabets, as every join is using a fresh feature name as parameter. This ensures that only one of the sequenced copies of  $s$ ,  $\overline{\alpha}_1(s, \theta)$  and  $\overline{\alpha}_2(s, \theta)$ , will actually be executed (and the other will amount to skip) in any given configuration of the product.

For sequential composition of abstractions  $\alpha_2 \circ \alpha_1$  we use the following rewrites:  $\alpha_2 \circ \alpha_1(\mathbb{F}) = \alpha_2(\alpha_1(\mathbb{F}))$ ,  $\alpha_2 \circ \alpha_1(\mathbb{K}) = \alpha_2(\alpha_1(\mathbb{K}))$  and  $\alpha_2 \circ \alpha_1(\# \text{if } (\theta) s) = \# \text{if } (\overline{\alpha}_2(\overline{\alpha}_1(\theta))) \overline{\alpha}_2(\overline{\alpha}_1(s, \theta), \overline{\alpha}_1(\theta))$ .



**Fig. 7.** Illustration of *derive* vs *abstract*:  $\overline{\mathcal{D}}_\alpha[s] = \overline{\mathcal{A}}[\alpha(s)]$ .

*Example 8.* Consider the program  $S'_1: \text{\#if}(A) \ x := x + 1; \text{\#if}(B) \ x := 1$  with  $\mathbb{F} = \{A, B\}$ ,  $\psi = A \vee B$ , and  $\mathbb{K}_\psi = \{A \wedge B, A \wedge \neg B, \neg A \wedge B\}$ . Then

$$\alpha_{Z'}^{\text{join}} \circ \alpha_A^{\text{proj}}(S'_1) = \text{\#if}(Z) \ x := x + 1; \text{\#if}(Z) \ \text{lub}(x := 1, \text{skip}) \quad (12)$$

The set of valid configurations after projection is changed to  $\{A \wedge B, A \wedge \neg B\}$ , and after join again to just  $\{Z\}$ . The obtained program has only one configuration, the one that satisfies  $Z$ . The projection does not change the statements of the program. The join rewrite however, simplifies the first **\#if** (it is statically determined; cf. the first case of  $\alpha_{Z'}^{\text{join}}$  transformation), and joins the second statement with **skip** as it is unknown whether it will be executed or not, in the lack of information about the assignment to  $B$  in the abstracted program. Note that since  $Z$  is the only one valid configuration, the obtained program is equivalent to:  $x := x + 1; \text{lub}(x := 1, \text{skip})$ . Similarly, we can calculate:  $\alpha_{Z'}^{\text{join}} \circ \alpha_B^{\text{proj}}(S'_1) = \text{\#if}(Z) \ \text{lub}(x := x + 1, \text{skip}); \text{\#if}(Z) \ x := 1$ .

Now consider  $((\alpha_{Z'}^{\text{join}} \circ \alpha_A^{\text{proj}}) \otimes \alpha_B^{\text{proj}})(S'_1)$ . The new set of features is  $\{Z, A, B\}$ . The subset  $\{A, B\}$  is retained from the right projection component, and  $\{Z\}$  comes from the left join-project component. After extending the configurations of both components with negations of absent feature names we get the following set of valid configurations:  $\mathbb{K}' = \{Z \wedge \neg A \wedge \neg B, \neg Z \wedge A \wedge B, \neg Z \wedge \neg A \wedge B\}$ . The result of the left join-project operand is the program (12), and the right rewrite (projection) never changes the statements, so its result is identical to  $S'_1$ . Thus we are composing programs (12) and  $S'_1$  using the parallel composition rewrites. Then  $((\alpha_{Z'}^{\text{proj}} \circ \alpha_A^{\text{join}}) \otimes \alpha_B^{\text{proj}})(S'_1)$  is:

$$\text{\#if}(Z \vee A) \ x := x + 1; \text{\#if}(Z) \ \text{lub}(x := 1, \text{skip}); \text{\#if}(B) \ x := 1$$

The first **\#if** has been unified using the first case of the transformation for  $\otimes$ , and the second **\#if** is transformed into two copies of the statement with different guards, using the second case of the rewrite definition. For any legal configuration in  $\mathbb{K}'$  at most one of them does not reduce to **skip**.  $\square$

Now the analysis  $\overline{\mathcal{A}}[\alpha(s)]$  and  $\overline{\mathcal{D}}_\alpha[s]$  coincide up to renaming of valid configurations. So the **reconfigurator** together with an existing implementation of  $\overline{\mathcal{A}}$  gives us the abstracted analysis  $\overline{\mathcal{D}}_\alpha$ . The above equality is illustrated by Fig. 1.

**Theorem 6.**

$\forall s \in \text{Stm}, \alpha : \mathbb{A}^{\mathbb{K}_\psi} \rightarrow \mathbb{A}^{\alpha(\mathbb{K}_\psi)} \in \text{Abs}, \bar{d} \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)} : \bar{\mathcal{D}}_\alpha[s] \bar{d} = \bar{\mathcal{A}}[\alpha(s)] \bar{d}$  <sup>5</sup>.

*Example 9.* Consider the program  $S_1$  from Example 1 with  $\mathbb{K}_\psi = \{A \wedge B, A \wedge \neg B, \neg A \wedge B\}$ . We have calculated in Example 7 that  $\bar{\mathcal{D}}_{\alpha^{\text{join}}} \llbracket S_1 \rrbracket ([x \mapsto \top]) = ([x \mapsto 1])$ . We now calculate  $\bar{\mathcal{A}}[\alpha_{A,Z}^{\text{join}}(S_1)]([x \mapsto \top])$  (here  $\alpha_{A,Z}^{\text{join}} = \alpha_{Z,Z}^{\text{join}} \circ \alpha_A^{\text{proj}}$ ):

$$([x \mapsto \top]) \xrightarrow{\bar{\mathcal{A}}[x:=0]} ([x \mapsto 0]) \xrightarrow{\bar{\mathcal{A}}[\text{if}(Z) x:=x+1]} ([x \mapsto 1]) \xrightarrow{\bar{\mathcal{A}}[\text{if}(Z) \text{ lub}(x:=1, \text{skip})]} ([x \mapsto 1])$$

## 6 Evaluation

Recall that there are two ways to speed up lifted analyses: improving *representation* and increasing *abstraction*. First, we will compare the performance of the two using an unoptimized lifted analysis as a baseline. Then, we demonstrate that abstraction may be used to turn previously infeasible analysis into feasible ones. Finally, we consider example scenarios that use projection and join and show that abstraction may be applied to an entire product line or when just analyzing a single method.

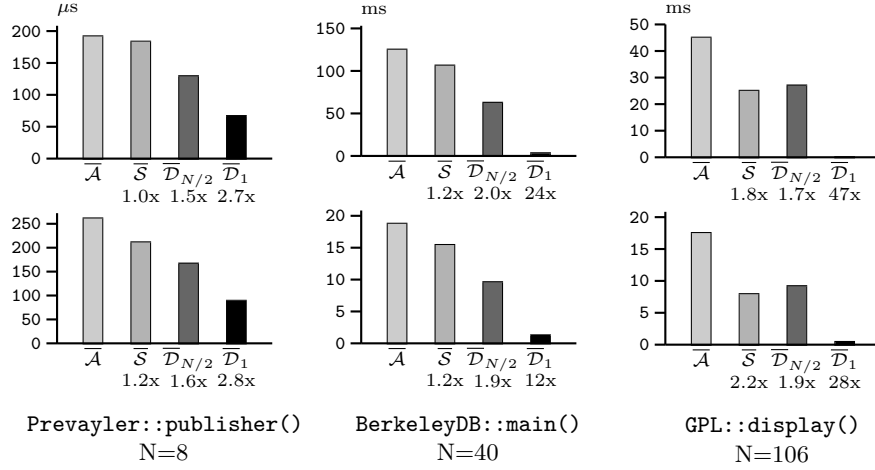
For our experiments, we use an existing implementation of lifted data-flow analyses for Java Object-Oriented SPLs [5]. The implementation is based on SOOT’s intra-procedural data-flow analysis framework [20] for analyzing Java programs. It uses CIDE (Colored IDE) [16] to annotate statements using background colors rather than `#ifdef` directives. Every feature is thus associated with a unique color.

We will consider an unoptimized lifted intra-procedural analysis, known as  $\mathcal{A}2$  (from [5]), that uses  $|\mathbb{K}_\psi|$ -tuples of analysis information, one analysis value per configuration. Also, we consider  $\mathcal{A}3$  (from [5]) which is the same analysis, but with improved representation via sharing of analysis-equivalent configurations using a high-performance bit vector library. Note that  $\mathcal{A}2$  corresponds to  $\bar{\mathcal{A}}$  in Fig. 2 and we will thus refer to it as  $\bar{\mathcal{A}}$ , while we will use  $\bar{\mathcal{S}}$  for the analysis with sharing ( $\mathcal{A}3$  in [5]). The performance of abstracted analyses depends on the size of tuples they work on. Therefore as variability abstractions, we have chosen  $\bar{\mathcal{D}}_{\alpha^{\text{join}}}$  which joins together (confounders) information from all configurations down to just one abstracted analysis value, and  $\bar{\mathcal{D}}_{\alpha_{N/2}^{\text{proj}} \otimes \alpha_{N/2}^{\text{join}}}$  (where  $N = |\mathbb{K}_\psi|$ ) which is a parallel composition of a projection of  $1/2$  (randomly selected) configurations and a *join* of the remaining  $1/2$  configurations. We abbreviate them as  $\bar{\mathcal{D}}_1$  and  $\bar{\mathcal{D}}_{N/2}$  in the following. We have chosen those variability abstractions because they represent the coarsest abstraction  $\bar{\mathcal{D}}_1$  that works on 1-sized tuples, and the medium abstraction  $\bar{\mathcal{D}}_{N/2}$  that works on  $N/2$ -sized tuples. Any other abstraction will have a speed up anywhere between  $\bar{\mathcal{A}}$  (no abstraction),  $\bar{\mathcal{D}}_{N/2}$  (medium abstraction) and  $\bar{\mathcal{D}}_1$  (maximum abstraction). It thus quantifies the potential of abstractions.

<sup>5</sup> The proof of this theorem is in App. F.

Benchmark	avg. $ \mathbb{K}_\psi $	$ \mathbb{F} $	LOC	max variability mth	$ \mathbb{K}_\psi $	$ \mathbb{F} $	LOC
Prevayler	N=1.3	5	8,000	P'F'.publisher()	N=8	3	10
BerkelyDB	N=1.6	42	84,000	DBRunAction.main()	N=40	7	165
GPL	N=3.9	18	1,350	Vertex.display()	N=106	9	31

**Fig. 8.** Characteristics of our three SPL benchmarks (average #configurations in all methods in SPL, total #features, and LOC) along with, for each SPL, its method with maximum variability (#configurations, local #features, and LOC).



**Fig. 9.** Analysis time for *reaching definitions* (above) and *uninitialized variables* (below):  $\bar{A}$  (baseline) and  $\bar{S}$  (sharing) vs.  $\bar{D}_{N/2}$  (medium abstraction) and  $\bar{D}_1$  (maximum abstraction).

For our experiment<sup>6</sup>, we have chosen two analyses: *reaching definitions* and *uninitialized variables*; and three SPL benchmarks [16]. Graph PL (GPL) is a small desktop application with intensive feature usage, Prevayler is a slightly larger product line with low feature usage, and BerkelyDB is a larger database library with moderate feature usage. Fig. 8 summarises relevant characteristics for each benchmark: the average number of valid configurations in all methods in the SPL, the total number of features in the entire SPL, the total number of lines of code (LOC). Also, for each SPL, the figure details information about the method with the highest variability (most configurations): its number of valid configurations, features, and lines of code.

*Performance.* Fig. 9 shows the time it takes to run each of our three maximum variability methods, as a relative comparison between  $\bar{A}$  (baseline) and  $\bar{S}$  (sharing)

<sup>6</sup> The implementation, benchmarks, and all results obtained from our experiments are available in the supplemental material submitted with this paper.

vs  $\overline{D}_{N/2}$  (medium abstraction) and  $\overline{D}_1$  (maximum abstraction). The experiments are executed on a 64-bit Intel®Core™ i5 CPU with 8 GB memory. All times are reported as averages over ten runs with the highest and lowest number removed. For each benchmark method, we give the speed up factor relative to the baseline (normalized with factor 1) and recall the number of configurations, N.

Our experiment confirms previous results that sharing is indeed effective and especially so for larger values of N [5]. On our methods, it translates to speed ups (i.e.,  $\overline{A}$  vs  $\overline{S}$ ) anywhere between 3% faster (for N=8) and slightly more than twice as fast (for N=106). We also observe that abstraction is not surprisingly significantly faster than unabridged analyses (i.e.,  $\overline{D}$  vs  $\overline{A}$  and  $\overline{S}$ ); i.e., abstraction yields significant performance gains, especially for benchmarks with higher variability. For GPL with N=106, we see a dramatic 47 and 28 times speed up depending on the analysis (i.e.,  $\overline{D}_1$  vs  $\overline{A}$ ). Also, we note that increased abstraction is up to 26 times faster than improved representation (i.e.,  $\overline{D}_1$  vs  $\overline{S}$ ). In general, it is obviously possible to combine the benefits from representation and abstraction to yield even more efficient analyses.

*From Infeasible to Feasible Analysis.* Of course, for very large values of N, analyses may become impractically slow or infeasible. As an experiment, we took a large method (`processFile()` from BerkeleyDB) and kept adding unconstrained variability. For  $N=2^{13}=8,192$  configurations, the analysis  $\overline{A}$  took 138 seconds. For  $N=2^{14}=16,384$ , it ran more than ten minutes until it eventually produced an out-of-memory error. In contrast, variability abstraction  $\overline{D}_1$  analyses the same high variability method in less than 8 ms (albeit less precisely). Hence, abstraction can not only speed up analyses, but also turn previously infeasible analyses feasible.

*Projection on Entire SPL.* GPL is a family of classical graph applications with variability on its representation and algorithms. For instance, the features `Directed` and `Undirected` control whether or not graphs are *directed*; `Weighted` and `Unweighted` control whether or not the graphs are *weighted*; and, the features `BFS` and `DFS` control the search algorithm used (*breadth-first search* or *depth-first search*). It is common industrial practice, to ship products with a subset of configurations, and thereby functionality. Here, we may use projection to *disable* features `BFS` and `Undirected`, along with any features that only work on undirected graphs: (`Connected`, `MSTKruskal`, and `MSTPrim` for implementing *connected components* and *minimum spanning trees* algorithms) which can be obtained from GPL’s feature model, detailing such feature dependencies. With this projection (abstraction), the configuration space of GPL is reduced from 528 to 370 valid configurations. This, in turn, cuts analysis time of reaching definitions in half (from 90ms to 49ms). For 123 out of 135 methods, the abstracted analysis computes the exact same analysis information. For larger product lines and projections, lots of time may be saved in this way.

*Join on One Method.* Figure 10 shows a fragment extracted from BerkeleyDB’s `main()` method with N=40 valid configurations. A local variable, `doAction` is

defined and initialized to zero, after which it is conditionally assigned three times in statements guarded by `#ifdefs`. (Actually, there are two more similar `#ifdefs` involving features `Evictor` and `DeleteOp`, but we have omitted those for brevity in the code fragment.) We can use a join abstraction of the reaching definitions analysis to compute what are the possible values (definitions) that *reach* the condition of the `switch` statement in line 12. An abstracted analysis would be able to determine that these are the assignments in lines 1, 3, 6, 8, and 10, by analyzing only *one* crudely over-approximated configuration instead of all ( $N=40$ ) configurations. In general, by inspecting the structure of the code and the features used, we can tailor abstractions that can analyze individual methods much faster than analyzing all configurations.

```

void main(..) {
1  .. int doAction = 0; ..
2  #ifdef Cleaner
3  if (..) doAction = CLEAN;
4  #endif
5  #ifdef INCompressor
6  if (..) doAction = COMPRESS;
7  #endif
8  if (..) doAction = CHECKPOINT;
9  #ifdef Statistics
10 if (..) doAction = DBSTATS;
11 #endif
12 .. switch (doAction) { .. } ..
}

```

**Fig. 10.** Code fragment extracted from `BerkeleyDB::main()` with  $N=40$ .

## 7 Related Work

Static analyses can be accelerated by devising more efficient representations or by introducing abstraction. In family-based analysis for software product lines the representation improvements primarily rely on sharing state information for variants with analysis-equivalent information (which implies reducing redundant computation). This can optimize the analyses considerably [5,6,14]. However, in the worst case, the number of variants that a lifted analysis has to consider is still inherently exponential in the number of features,  $|\mathbb{F}|$ . Thus with a large number of features lifted analyses may become impractical or even infeasible. In this work we have taken the alternate route of using abstraction. Our experiments show that abstraction introduces speed-ups independently of representation gains. Thus our results can be beneficially combined with efficient representations.

An efficient implementation of lifted analysis formulated within the IFDS framework [18] for inter-procedural distributive environments was proposed in  $\text{SPL}^{\text{LIFT}}$  [4]. It uses binary decision diagrams to represent shared feature constraints. The authors have found that the running time of analysing all variants in a family is close to the analysis of a single-program. In such case, further

benefit of applying abstraction, as presented in this paper, is unlikely to bring any significant improvement. However, notice that the method of  $\text{SPL}^{\text{LIFT}}$  is limited only to distributive data-flow analysis encoded within the IFDS framework. Many analyses, including constant propagation, are not distributive and hence cannot be expressed in IFDS. Let alone static analyses that are not expressible as data-flow analyses (including type checking, model-checking, etc).

The formal developments in this paper are based on *variational abstract interpretation*, a formal methodology for systematic derivation of lifted analyses for `#ifdef`-based product lines, proposed in [17]. The method is based on the calculational approach to abstract interpretation of Cousot [11], applied and contextualized to product lines. In that work, Galois connections are not used for lifting, but only for derivation of single program analyses as shown in [11], so they are variability-unaware. Calculations are used to derive a directly operational *abstracted lifted analysis* which is *correct* by construction. In the present paper, we assume that lifted analyses exist (possibly obtained using the methodology of [17]), and focus on abstracting variability using them. We devise an expressive calculus for specifying abstraction operators. Also, thanks to our tool, all abstractions specifiable in our calculus, are now automatically executable.

A good collection of analyses that have been lifted manually is presented in the survey [19]. We should remark, that the join operation  $\alpha^{\text{join}}$  allows applying single program analyses to program families, even if with precision loss. In that sense, the our approach is the first ever method that can *automatically* lift single program analyses to work on program families. Besides the family-based strategy, the survey [19] identifies a *sampling strategy* as a suitable way of analyzing product lines (see also [1]). In the sampling strategy only a random subset of products is analyzed. We remark that once the sample is selected, our projection operator  $\alpha_{\varphi}^{\text{fproj}}$  can be used to realize the sampling strategy in a simultaneous way by exploiting an existing family-based analysis.

In fact, the algebraic specification framework of Section 3 allows specifying any analysis in the spectrum between a fully family-based analyses, and a single variant, *product-based*, analysis. We can specify abstractions that select (sample) any subsets of configurations and then analyze this subset with selected choice of precision, either all variants precisely, like in sampling, or confounding some executions for efficiency. In this sense, we show how to design analyses placed anywhere in the design spectrum painted in [19]. Consider, the *feature-based* analysis strategy as an example. In this strategy an analysis explores the program code feature-by-feature (as opposed to configuration-by-configuration). Analyses following this strategy can now be systematically obtained using our abstractions, by projecting away (ignoring) all but one feature and running a single program analysis on the result. This is quite remarkable. It has been well recognized that designing such analyses is very difficult, yet now there exists a systematic way of doing that, so it is no longer an impenetrable art.



## 8 Conclusion

We have defined variability-aware abstractions given as Galois connections, and used them to derive efficient and correct-by-construction abstract analyses of program families. We have designed a calculus for the abstractions, and shown how abstractions specified in this language can be applied not only on analyses, but also on programs, obtaining a convenient implementation strategy of the abstractions in form of a source-to-source **reconfigurator** transformation.

The **reconfigurator** transformation presently requires that the programming language is able to express *sequential composition* (e.g., “;” in IMP) and *join of statements* (i.e., **lub** as in “ $\sqcup$ ”) with respect to the analysis in question. It would be interesting to consider lifting those assumptions in future, and apply this method to more modeling and programming languages.

We evaluated the method on three Java-based product lines. We found that the abstractions improve performance of analyses independently of improvements in the data representations used in the implementations of these analyses. This indicates that the proposed abstraction strategies will be instrumental in tackling error finding analysis in large configurable software systems, like the Linux kernel. Indeed we have developed these techniques with the intention of scaling error finding tools to such challenging cases in future. Besides this, we would like to experiment with applying these abstraction techniques to alternative quality assurance methods including model checking, and testing.

## References

1. S. Apel, A. von Rhein, P. Wendler, A. Groslinger, D. Beyer. Strategies for product-line verification: case studies and experiments. In: 35th International Conference on Software Engineering, ICSE’13, 2013, pp. 482–491.
2. D. Batory. Feature Models, Grammars, and Propositional Formulas. In: Obbink, J. H. and Pohl, K. (eds.) SPLC 2006. LNCS vol. 3714, pp. 7–20. Springer, 2006.
3. T. Berger, D. Nair, R. Rublack, J. M. Atlee, K. Czarnecki, A. Wasowski. Three cases of feature-based variability modeling in industry In: MODELS 2014, 2014, pp. 302–319.
4. E. Bodden, T. Tolêdo, M. Ribeiro, C. Brabrand, P. Borba, M. Mezini. SPL<sup>LIFT</sup> - Statically Analyzing Software Product Lines in Minutes Instead of Years. In: Proc. ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), 2013, pp. 355–364.
5. C. Brabrand, M. Ribeiro, T. Tolêdo, J. Winther, P. Borba. Intraprocedural dataflow analysis for software product lines. In: Transactions on Aspect-Oriented Software Development 10, 2013, pp. 73–108.
6. A. Classen, P. Heymans, P.-Y. Schobbens, A. Legay. Symbolic model checking of software product lines. In: ICSE’11, 2011, pp. 321–330.
7. P. Clements, L. Northrop. *Software Product Lines: Practices and Patterns*. Addison-Wesley, 2001.
8. P. Cousot, R. Cousot. Systematic design of program analysis frameworks. In: POPL’79, 1979, pp. 269–282.
9. P. Cousot, R. Cousot. Abstract interpretation and application to logic programs. In: Journal of Logic Programming 13 (2–3) (1992) 103–179.

10. P. Cousot. Types as abstract interpretations. In: POPL'97, 1997, pp. 316–331.
11. P. Cousot. The Calculational Design of a Generic Abstract Interpreter. Calculational System Design, NATO ASI Series F. IOS Press, 1999.
12. P. Cousot, R. Cousot. Refining model checking by abstract interpretation. Autom. Softw. Eng. 6 (1) (1999) 69–95.
13. D. Guilbaud, E. Goubault, A. Pacalet, B. S. F. Védryne. A simple abstract interpreter for threat detection and test case generation. In: WAPATV'01, with ICSE'01, Toronto, 2001.
14. C. Kästner, S. Apel, Thomas Thüm, Gunter Saake. Type checking annotation-based product lines. ACM Transactions on Software Engineering and Methodology. Volume 21 Issue 3, June 2012.
15. C. Kästner, S. Apel, M. Kuhlemann. Granularity in software product lines. In: Schafer, W., Dwyer, M.B., Gruhn, V. (eds.), ICSE'08. ACM, pp. 311–320, 2008.
16. C. Kästner. *Virtual Separation of Concerns: Toward Preprocessors 2.0*. PhD thesis, University of Magdeburg, 2010.
17. J. Midtgaard, C. Brabrand, and A. Wasowski. Systematic Derivation of Static Analyses for Software Product Lines. In: 13th Int'l Conference on Modularity, 2014.
18. T. Reps, S. Horwitz, M. Sagiv. Precise interprocedural dataflow analysis via graph reachability. In: Proc. 22nd POPL '95, 1995, pp. 49–61.
19. T. Thüm, S. Apel, C. Kästner, I. Schaefer, G. Saake. A classification and survey of analysis strategies for software product lines. In ACM Comput. Surv. 47(1), 2014.
20. R. Vallee-Rai, P. Co, E. Gagnon, L. J. Hendren, P. Lam, V. Sundaresan. Soot - a Java bytecode optimization framework. In: MacKay, S. A., and Johnson, J. H. (eds.), CASCON 1999. IBM, pp. 13, (1999).
21. G. Winskel. *The Formal Semantics of Programming Languages*. Foundation of Computing Series, The MIT Press, 1993.

## A Properties of Abstraction Operators

We recall properties of Galois connections for completeness.

A pair  $\langle L, \leq_L \rangle \xrightleftharpoons[\alpha]{\gamma} \langle M, \leq_M \rangle$  is a *Galois connection* between complete lattices  $L$  and  $M$  iff  $\alpha$  and  $\gamma$  are total functions that satisfy:  $\alpha(l) \leq_M m \iff l \leq_L \gamma(m)$  for all  $l \in L, m \in M$ .

Some important properties of Galois connections [9] include: 1)  $\gamma \circ \alpha$  is *extensive*, i.e.  $l \leq_L (\gamma \circ \alpha)(l)$  for all  $l \in L$ ; 2)  $\alpha \circ \gamma$  is *reductive*, i.e.  $(\alpha \circ \gamma)(m) \leq_M m$  for all  $m \in M$ ; 3)  $\alpha$  is a *complete join morphism* (CJM), i.e.  $\alpha(\bigsqcup_{l \in L'} l) = \bigsqcup_{l \in L'} \alpha(l)$  for all  $L' \subseteq L$ .

Now we turn to proving theorems of Sect. 3.1.

*Proof (Thm. 1).* Let  $\bar{a} \in \mathbb{A}^{\mathbb{K}}$  and  $a \in \mathbb{A}^{\alpha^{\text{join}}(\mathbb{K})} \equiv \mathbb{A}$ ; recall that  $\alpha^{\text{join}}(\mathbb{K})$  is always a singleton. We have:

$$\begin{aligned}
 \alpha^{\text{join}}(\bar{a}) &\dot{\sqsubseteq} (a) \\
 \iff (\bigsqcup_{k \in \mathbb{K}} \pi_k(\bar{a})) &\sqsubseteq (a) && \text{(by def. of } \alpha^{\text{join}}) \\
 \iff \forall k \in \mathbb{K}. \pi_k(\bar{a}) &\sqsubseteq a && \text{(by def. of } \sqcup) \\
 \iff \bar{a} \dot{\sqsubseteq} \gamma^{\text{join}}(a) &&& \text{(by def. of } \gamma^{\text{join}})
 \end{aligned}$$

□

*Proof (Thm. 2).* Let  $\bar{a} \in \mathbb{A}^{\mathbb{K}}$  and  $\bar{a}' \in \mathbb{A}^{\{k \in \mathbb{K} \mid k \models \varphi\}}$ . We have:

$$\begin{aligned}
 \alpha_{\varphi}^{\text{proj}}(\bar{a}) &\dot{\sqsubseteq} \bar{a}' \\
 \iff \forall k \in \mathbb{K}. k \models \varphi. \pi_k(\bar{a}) &\sqsubseteq \pi_k(\bar{a}') && \text{(by def. of } \alpha_{\varphi}^{\text{proj}}) \\
 \iff \forall k \in \mathbb{K}. k \models \varphi. \pi_k(\bar{a}) &\sqsubseteq \pi_k(\bar{a}') \wedge \forall k \in \mathbb{K}. k \not\models \varphi. \pi_k(\bar{a}) \sqsubseteq \top && \text{(by def. of } \sqcup) \\
 \iff \bar{a} \dot{\sqsubseteq} \gamma_{\varphi}^{\text{proj}}(\bar{a}') &&& \text{(by def. of } \gamma_{\varphi}^{\text{proj}})
 \end{aligned}$$

□

For sequential composition Galois connection properties follow directly from the definition and the standard results about compositions of Galois connections. Let's consider the parallel composition:

*Proof (Thm. 3).* To verify that this defines a Galois connection, we calculate:

$$\begin{aligned}
 \alpha_1 \otimes \alpha_2(\bar{a}) &\dot{\sqsubseteq} \bar{a}' \\
 \iff \alpha_1(\bar{a}) \times \alpha_2(\bar{a}) &\dot{\sqsubseteq} \bar{a}' && \text{(by def. of } \alpha_1 \otimes \alpha_2) \\
 \iff \alpha_1(\bar{a}) \dot{\sqsubseteq} \pi_{\alpha_1(\mathbb{K})}(\bar{a}') \wedge \alpha_2(\bar{a}) &\dot{\sqsubseteq} \pi_{\alpha_2(\mathbb{K})}(\bar{a}') && \text{(by def. of } \bar{a}_1 \times \bar{a}_2, \pi_{\alpha_1(\mathbb{K})}, \text{ and } \pi_{\alpha_2(\mathbb{K})}) \\
 \iff \bar{a} \dot{\sqsubseteq} \gamma_1(\pi_{\alpha_1(\mathbb{K})}(\bar{a}')) \wedge \bar{a} &\dot{\sqsubseteq} \gamma_2(\pi_{\alpha_2(\mathbb{K})}(\bar{a}')) && \text{(by def. of Galois conn.)} \\
 \iff \bar{a} \dot{\sqsubseteq} \gamma_1(\pi_{\alpha_1(\mathbb{K})}(\bar{a}')) \sqcap \gamma_2(\pi_{\alpha_2(\mathbb{K})}(\bar{a}')) &&& \text{(by def. of } \sqcap) \\
 \iff \bar{a} \dot{\sqsubseteq} \gamma_1 \otimes \gamma_2(\bar{a}') &&& \text{(by def. of } \gamma_1 \otimes \gamma_2)
 \end{aligned}$$

We now turn our attention to proving properties of the derived abstraction operators introduced in Sect. 3.2. Observe that all derived abstractions are Galois connections thanks to theorems of Sect. 3.1.

We proceed to show that  $\alpha_A^{\text{fgnore}}$  can be expressed using the basic abstractions. This will allow us to disregard it in further proofs, which are mostly done by structural induction on the structure of the abstractions. In this proof, it is convenient to name the configuration formulas of the abstract domain, so let  $\{k'_1, \dots, k'_n\} = \alpha_A^{\text{fgnore}}(\mathbb{K})$ , indexed in the order of components in vectors indexed by  $\alpha_A^{\text{fgnore}}(\mathbb{K})$ . Also, recall that  $\alpha_\varphi^{\text{join}} = \alpha^{\text{join}} \circ \alpha_\varphi^{\text{proj}}$  is another derived operator, which we use in this theorem.

*Proof (Thm. 4).* We first look into the expansion of  $\alpha_A^{\text{fgnore}}$  and establish that the types of both sides are correct. By definition (equation (10)) the type of  $\alpha_A^{\text{fgnore}}$  is  $\mathbb{A}^{\mathbb{K}} \rightarrow \mathbb{A}^{\{k'_1, \dots, k'_n\}}$ . The type of each  $\alpha_{k'_i}^{\text{join}}$  in the right hand side of the equality is  $\mathbb{A}^{\mathbb{K}} \rightarrow \mathbb{A}^{\{k'_i\}}$ , and consequently the type of the entire product in the left-hand-side is  $\mathbb{A}^{\mathbb{K}} \rightarrow \mathbb{A}^{\{k'_1, \dots, k'_n\}}$  as required; cf. the definition of parallel composition for configuration sets.

The proof proceeds by mathematical induction with the following hypothesis:

$$\left( \alpha_{k'_1}^{\text{join}} \otimes \dots \otimes \alpha_{k'_i}^{\text{join}} \right) (\bar{a}) = \prod_{l=1}^i \bigsqcup_{k \in \mathbb{K}, k \models k'_l} \pi_k(\bar{a}) \quad (13)$$

*Base case.* Consider a single  $\alpha_{k'_i}^{\text{join}}$  and let  $\bar{a} \in \mathbb{A}^{\mathbb{K}}$ . We proceed by equational reasoning from left to right:

$$\begin{aligned} \alpha_{k'_i}^{\text{join}}(\bar{a}) &= (\alpha^{\text{join}} \circ \alpha_{k'_i}^{\text{proj}})(\bar{a}) && \text{(def. of } \alpha_\varphi^{\text{join}}) \\ &= \alpha^{\text{join}} \left( \prod_{\{k \in \mathbb{K} \mid k \models k'_i\}} \pi_k(\bar{a}) \right) && \text{(def. of } \alpha_\varphi^{\text{proj}}) \\ &= \left( \bigsqcup_{\{k \in \mathbb{K} \mid k \models k'_i\}} \pi_k(\bar{a}) \right) && \text{(def. of } \alpha^{\text{join}}) \end{aligned}$$

*Inductive step* (again by equational reasoning from left to right):

$$\begin{aligned} &\left( \alpha_{k'_1}^{\text{join}} \otimes \dots \otimes \alpha_{k'_{i+1}}^{\text{join}} \right) (\bar{a}) = \\ &= \left( \left( \lambda \bar{a}. \prod_{l=1}^i \bigsqcup_{k \in \mathbb{K}, k \models k'_l} \pi_k(\bar{a}) \right) \otimes \alpha_{k'_{i+1}}^{\text{join}} \right) (\bar{a}) && \text{(by IH)} \\ &= \left( \left( \lambda \bar{a}. \prod_{l=1}^i \bigsqcup_{k \in \mathbb{K}, k \models k'_l} \pi_k(\bar{a}) \right) \otimes \left( \lambda \bar{a}. \left( \bigsqcup_{k \in \mathbb{K}, k \models k'_{i+1}} \pi_k(\bar{a}) \right) \right) \right) (\bar{a}) \\ &\quad \text{(the base case above)} \\ &= \left( \lambda \bar{a}. \prod_{l=1}^{i+1} \bigsqcup_{k \in \mathbb{K}, k \models k'_l} \pi_k(\bar{a}) \right) (\bar{a}) \\ &\quad \text{(def. of } \otimes; k'_{i+1} \text{ is a different formula from any of } k'_l\text{'s)} \\ &= \prod_{l=1}^{i+1} \bigsqcup_{k \in \mathbb{K}, k \models k'_l} \pi_k(\bar{a}) && \text{(beta reduction)} \end{aligned}$$

The above completes the inductive proof. The inductive hypothesis for  $i = n$  concludes the proof of correctness for expansion of  $\alpha_A^{\text{fgnore}}$ .

The proof for the expansion of  $\gamma_A^{\text{fignore}}$  is similar. The type of  $\gamma_A^{\text{fignore}}$  is by definition  $\mathbb{A}^{\{k'_1, \dots, k'_n\}} \rightarrow \mathbb{A}^{\mathbb{K}}$ . The type of each of the factors in the right-hand-side is  $\gamma_{k'_l}^{\text{join}} : \mathbb{A}^{\{k'_l\}} \rightarrow \mathbb{A}^{\mathbb{K}}$ . Now, by definition of the product the type of the entire term is:  $\mathbb{A}^{\{k'_1, \dots, k'_n\}} \rightarrow \mathbb{A}^{\mathbb{K}}$  (since  $k'_l$  are different formulae).  
The inductive hypothesis is ( $\bar{a}'' \in \mathbb{A}^{\{k'_1, \dots, k'_i\}}$ ):

$$\left( \gamma_{k'_1}^{\text{join}} \otimes \dots \otimes \gamma_{k'_i}^{\text{join}} \right) (\bar{a}'') = \prod_{k \in \mathbb{K}} \begin{cases} \pi_{k'_l}(\bar{a}'') & \text{if } k \models k'_l \text{ for some } l \in 1..i \\ \top & \text{otherwise} \end{cases}$$

*Base case.*

$$\begin{aligned} \gamma_{k'_l}^{\text{fignore}} &= \gamma_{k'_l}^{\text{proj}} \circ \gamma_{k'_l}^{\text{join}} = \gamma_{k'_l}^{\text{proj}} \circ (\lambda \bar{a}'' . \prod_{k \in \mathbb{K}, k \models k'_l} \pi_{k'_l}(\bar{a}'')) \\ &= \left( \lambda \bar{a}' . \prod_{k \in \mathbb{K}} \begin{cases} \pi_{k'_l}(\bar{a}') & \text{if } k \models k'_l \\ \top & \text{otherwise} \end{cases} \right) \circ (\lambda \bar{a}'' . \prod_{k \in \mathbb{K}, k \models k'_l} \pi_{k'_l}(\bar{a}'')) \\ &\quad \text{(def. of projection)} \\ &= \lambda \bar{a}'' . \prod_{k \in \mathbb{K}} \begin{cases} \pi_{k'_l}(\bar{a}'') & \text{if } k \models k'_l \\ \top & \text{otherwise} \end{cases} \quad \text{(composition)} \end{aligned}$$

*Inductive step.*

$$\begin{aligned} &\left( \gamma_{k'_1}^{\text{join}} \otimes \dots \otimes \gamma_{k'_{i+1}}^{\text{join}} \right) (\bar{a}'') = \left( (\gamma_{k'_1}^{\text{join}} \otimes \dots \otimes \gamma_{k'_i}^{\text{join}}) \otimes \gamma_{k'_{i+1}}^{\text{join}} \right) (\bar{a}'') \\ &= \left( \lambda \bar{a}'' . \left( \prod_{k \in \mathbb{K}} \begin{cases} \pi_{k'_l}(\bar{a}'') & \text{if } k \models k'_l \text{ for some } l \in 1..i \\ \top & \text{otherwise} \end{cases} \right) \otimes \right. \\ &\quad \left. \left( \prod_{k \in \mathbb{K}} \begin{cases} \pi_{k'_{i+1}}(\bar{a}'') & \text{if } k \models k'_{i+1} \\ \top & \text{otherwise} \end{cases} \right) \right) (\bar{a}'') \quad \text{(IH and the base case)} \\ &= \left( \lambda \bar{a}'' . \prod_{k \in \mathbb{K}} \begin{cases} \pi_{k'_l}(\bar{a}'') & \text{if } k \models k'_l \text{ for some } l \in 1..i+1 \\ \top & \text{otherwise} \end{cases} \right) (\bar{a}'') \\ &\quad \text{(} k'_l \text{ formulas are not equivalent and } \otimes \text{ uses } \sqcup \text{)} \\ &= \prod_{k \in \mathbb{K}} \begin{cases} \pi_{k'_l}(\bar{a}'') & \text{if } k \models k'_l \text{ for some } l \in 1..i+1 \\ \top & \text{otherwise} \end{cases} \quad \text{(beta reduction)} \end{aligned}$$

Now, instantiate the inductive hypothesis for  $i = n$ , and observe that for any  $k \in \mathbb{K}$  there exists a  $k'_l \in \alpha_{\mathbb{K}}^{\text{fignore}}$ , such that  $k \models k'_l$ , so the second case is never exercised and we end up concluding that:

$$\left( \gamma_{k'_1}^{\text{join}} \otimes \dots \otimes \gamma_{k'_n}^{\text{join}} \right) (\bar{a}'') = \gamma_A^{\text{fignore}}(\bar{a}'')$$

□

## B Appendix: Proof of Soundness of Abstracted Analyses

We denote with  $(*)$  the equation:

$$\alpha(\bar{a}) = \prod_{k' \in \alpha(\mathbb{K})} \pi_{k'}(\alpha(\bar{a}))$$

where  $\bar{a} \in \mathbb{A}^{\mathbb{K}}$  and  $\alpha : \mathbb{A}^{\mathbb{K}} \rightarrow \mathbb{A}^{\alpha(\mathbb{K})} \in Abs$ .

**Proposition 1.**  $\forall e \in Exp, (\alpha, \gamma) \in Abs, \bar{d} \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)} : \alpha \circ \overline{\mathcal{A}'}[e] \circ \gamma(\bar{d}) \sqsubseteq \overline{\mathcal{D}'}_\alpha[e] \bar{d}$

*Proof.* By induction on the structure of expressions.

**Case  $n$ :**

$$\begin{aligned} & (\alpha \circ \overline{\mathcal{A}'}[n] \circ \gamma)(\bar{d}) \\ &= \alpha(\overline{\mathcal{A}'}[n](\gamma(\bar{d}))) && \text{(by def. of } \circ) \\ &= \alpha\left(\prod_{k \in \mathbb{K}_\psi} n\right) && \text{(by def. of } \overline{\mathcal{A}'} \text{ in Fig. 2)} \\ &= \prod_{k' \in \alpha(\mathbb{K}_\psi)} n && \text{(by helper Lemma 1 in App. C)} \\ &= \overline{\mathcal{D}'}_\alpha[n] \end{aligned}$$

**Case  $\mathbf{x}$ :**

$$\begin{aligned} & (\alpha \circ \overline{\mathcal{A}'}[\mathbf{x}] \circ \gamma)(\bar{d}) \\ &= \alpha(\overline{\mathcal{A}'}[\mathbf{x}](\gamma(\bar{d}))) && \text{(by def. of } \circ) \\ &= \alpha\left(\prod_{k \in \mathbb{K}_\psi} \pi_k(\gamma(\bar{d}))(\mathbf{x})\right) && \text{(by def. of } \overline{\mathcal{A}'} \text{ in Fig. 2)} \\ &= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\alpha(\gamma(\bar{d}))(\mathbf{x})) && \text{(by def. of } (*)) \\ &\sqsubseteq \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\bar{d})(\mathbf{x}) && \text{(\alpha } \circ \gamma \text{ is reductive)} \\ &= \overline{\mathcal{D}'}_\alpha[\mathbf{x}] \bar{d} \end{aligned}$$

**Case  $e_0 \oplus e_1$ :**

$$\begin{aligned}
& (\alpha \circ \overline{\mathcal{A}}[e_0 \oplus e_1] \circ \gamma)(\bar{d}) \\
&= \alpha(\overline{\mathcal{A}}[e_0 \oplus e_1](\gamma(\bar{d}))) && \text{(by def. of } \circ \text{)} \\
&= \alpha\left(\prod_{k \in \mathbb{K}_\psi} \pi_k(\overline{\mathcal{A}}[e_0]\gamma(\bar{d})) \hat{\oplus} \pi_k(\overline{\mathcal{A}}[e_1]\gamma(\bar{d}))\right) && \text{(by def. of } \overline{\mathcal{A}} \text{ in Fig. 2)} \\
&= \alpha\left(\prod_{k \in \mathbb{K}_\psi} \pi_k(\overline{\mathcal{A}}[e_0]\gamma(\bar{d}) \hat{\oplus} \overline{\mathcal{A}}[e_1]\gamma(\bar{d}))\right) && \text{(by def. of } \pi_k \text{ and } \hat{\oplus} \text{)} \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\alpha(\overline{\mathcal{A}}[e_0]\gamma(\bar{d}) \hat{\oplus} \overline{\mathcal{A}}[e_1]\gamma(\bar{d}))) && \text{(by def. of } (*) \text{)} \\
&\stackrel{\cdot}{\subseteq} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\alpha(\overline{\mathcal{A}}[e_0]\gamma(\bar{d})) \hat{\oplus} \alpha(\overline{\mathcal{A}}[e_1]\gamma(\bar{d}))) \\
&\hspace{15em} \text{(by helper Lemma 3 in App. C)} \\
&\stackrel{\cdot}{\subseteq} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\overline{\mathcal{D}}'_\alpha[e_0]\bar{d} \hat{\oplus} \overline{\mathcal{D}}'_\alpha[e_1]\bar{d}) && \text{(by IH, twice)} \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\overline{\mathcal{D}}'_\alpha[e_0]\bar{d}) \hat{\oplus} \pi_{k'}(\overline{\mathcal{D}}'_\alpha[e_1]\bar{d}) && \text{(by def. of } \pi_{k'} \text{ and } \hat{\oplus} \text{)} \\
&= \overline{\mathcal{D}}'_\alpha[e_0 \oplus e_1]\bar{d}
\end{aligned}$$

**Proposition 2.**  $\forall s \in Stm, (\alpha, \gamma) \in Abs, \bar{d} \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)} : \alpha \circ \overline{\mathcal{A}}[s] \circ \gamma(\bar{d}) \stackrel{\cdot}{\subseteq} \overline{\mathcal{D}}_\alpha[s]\bar{d}$

*Proof.* By induction on the structure of statements. First, we define  $\bar{d}[\mathbf{x} \mapsto \bar{v}] = \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\bar{d})[\mathbf{x} \mapsto \pi_{k'}(\bar{v})]$ , for all  $\bar{d} \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)}$  and  $\bar{v} \in Const^{\alpha(\mathbb{K}_\psi)}$ . Thus,  $\bar{d}[\mathbf{x} \mapsto \bar{v}]$  is a tuple that is as  $\bar{d}$  except that in each component of  $\bar{d}$  the variable  $\mathbf{x}$  is mapped to the corresponding component of the tuple  $\bar{v}$ .

**Case skip:**

$$\begin{aligned}
& (\alpha \circ \overline{\mathcal{A}}[\text{skip}] \circ \gamma)(\bar{d}) \\
&= \alpha(\overline{\mathcal{A}}[\text{skip}](\gamma(\bar{d}))) && \text{(by def. of } \circ \text{)} \\
&= \alpha(\gamma(\bar{d})) && \text{(by def. of } \overline{\mathcal{A}} \text{ in Fig. 2)} \\
&\stackrel{\cdot}{\subseteq} \bar{d} && \text{(\(\alpha \circ \gamma\) is reductive)} \\
&= \overline{\mathcal{D}}_\alpha[\text{skip}]\bar{d}
\end{aligned}$$

**Case  $x := e$ :**

$$\begin{aligned}
& (\alpha \circ \overline{\mathcal{A}}[\mathbf{x} := e] \circ \gamma)(\overline{d}) \\
&= \alpha \left( \prod_{k \in \mathbb{K}_\psi} \pi_k(\gamma(\overline{d}))[\mathbf{x} \mapsto \pi_k(\overline{\mathcal{A}}'[e]\gamma(\overline{d}))] \right) && \text{(by def. of } \overline{\mathcal{A}} \text{ in Fig. 2)} \\
&= \alpha \left( \prod_{k \in \mathbb{K}_\psi} \pi_k(\gamma(\overline{d}))[\mathbf{x} \dot{\mapsto} \overline{\mathcal{A}}'[e]\gamma(\overline{d})] \right) && \text{(by def. of } \dot{\mapsto} \text{)} \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\alpha(\gamma(\overline{d}))[\mathbf{x} \dot{\mapsto} \overline{\mathcal{A}}'[e]\gamma(\overline{d})]) && \text{(by def. of } (*) \text{)} \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\alpha(\gamma(\overline{d}))[\mathbf{x} \dot{\mapsto} \alpha(\overline{\mathcal{A}}'[e]\gamma(\overline{d}))]) \\
&\hspace{15em} \text{(by helper Lemma 4 in App. C)} \\
&\stackrel{\dot{=}}{=} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\overline{d}[\mathbf{x} \dot{\mapsto} \overline{\mathcal{D}}'_\alpha[e]\overline{d}]) && \text{(IH, and } \alpha \circ \gamma \text{ is reductive)} \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\overline{d})[\mathbf{x} \mapsto \pi_{k'}(\overline{\mathcal{D}}'_\alpha[e]\overline{d})] && \text{(by def. of } \dot{\mapsto} \text{)} \\
&= \overline{\mathcal{D}}_\alpha[\mathbf{x} := e]\overline{d}
\end{aligned}$$

**Case  $\text{if } e \text{ then } s_0 \text{ else } s_1$ :**

$$\begin{aligned}
& (\alpha \circ \overline{\mathcal{A}}[\text{if } e \text{ then } s_0 \text{ else } s_1] \circ \gamma)(\overline{d}) \\
&= \alpha(\overline{\mathcal{A}}[\text{if } e \text{ then } s_0 \text{ else } s_1](\gamma(\overline{d}))) && \text{(by def. of } \circ \text{)} \\
&= \alpha(\overline{\mathcal{A}}[s_0]\gamma(\overline{d}) \dot{\cup} \overline{\mathcal{A}}[s_1]\gamma(\overline{d})) && \text{(by def. of } \overline{\mathcal{A}} \text{ in Fig. 2)} \\
&= \alpha(\overline{\mathcal{A}}[s_0]\gamma(\overline{d})) \dot{\cup} \alpha(\overline{\mathcal{A}}[s_1]\gamma(\overline{d})) && \text{(by } \alpha \text{ is a CJM)} \\
&\stackrel{\dot{=}}{=} \overline{\mathcal{D}}_\alpha[s_0]\overline{d} \dot{\cup} \overline{\mathcal{D}}_\alpha[s_1]\overline{d} && \text{(by IH, twice)} \\
&= \overline{\mathcal{D}}_\alpha[\text{if } e \text{ then } s_0 \text{ else } s_1]\overline{d}
\end{aligned}$$



**Case #if ( $\theta$ )  $s$ :**

$$\begin{aligned}
& (\alpha \circ \overline{\mathcal{A}}[\text{\#if } (\theta) s] \circ \gamma)(\bar{d}) \\
&= \alpha(\overline{\mathcal{A}}[\text{\#if } (\theta) s](\gamma(\bar{d}))) && \text{(by def. of } \circ \text{)} \\
&= \alpha\left(\prod_{k \in \mathbb{K}_\psi} \begin{cases} \pi_k(\overline{\mathcal{A}}[s]\gamma(\bar{d})) & \text{if } k \models \theta \\ \pi_k(\gamma(\bar{d})) & \text{if } k \not\models \theta \end{cases}\right) && \text{(by def. of } \overline{\mathcal{A}} \text{ in Fig. 2)} \\
&\stackrel{\dot{=}}{=} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\alpha(\overline{\mathcal{A}}[s]\gamma(\bar{d}))) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha(\gamma(\bar{d}))) \sqcup \pi_{k'}(\alpha(\overline{\mathcal{A}}[s]\gamma(\bar{d}))) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg\theta) \\ \pi_{k'}(\alpha(\gamma(\bar{d}))) & \text{if } k' \models \neg\theta \end{cases} && \text{(by helper Lemma 2 in App. C)} \\
&\stackrel{\dot{=}}{=} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_\alpha[s]\bar{d}) & \text{if } k' \models \theta \\ \pi_{k'}(\bar{d}) \sqcup \pi_{k'}(\overline{\mathcal{D}}_\alpha[s]\bar{d}) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg\theta) \\ \pi_{k'}(\bar{d}) & \text{if } k' \models \neg\theta \end{cases} && \text{(by IH, and } \alpha \circ \gamma \text{ is reductive)} \\
&= \overline{\mathcal{D}}_\alpha[\text{\#if } (\theta) s] \bar{d}
\end{aligned}$$

**Case while  $e$  do  $s$ :** We introduce a higher-order Galois connection between  $\mathbb{A}^{\mathbb{K}_\psi} \rightarrow \mathbb{A}^{\mathbb{K}_\psi}$  and  $\mathbb{A}^{\alpha(\mathbb{K}_\psi)} \rightarrow \mathbb{A}^{\alpha(\mathbb{K}_\psi)}$  defined as:

$$\begin{aligned}
\alpha_{\rightarrow}(\overline{\Phi}) &= \lambda \bar{d}. \alpha(\overline{\Phi}(\gamma(\bar{d}))), \text{ for } \overline{\Phi} : \mathbb{A}^{\mathbb{K}_\psi} \rightarrow \mathbb{A}^{\mathbb{K}_\psi} \\
\gamma_{\rightarrow}(\overline{\Phi'}) &= \lambda \bar{a}. \gamma(\overline{\Phi'}(\alpha(\bar{a}))), \text{ for } \overline{\Phi'} : \mathbb{A}^{\alpha(\mathbb{K}_\psi)} \rightarrow \mathbb{A}^{\alpha(\mathbb{K}_\psi)}
\end{aligned}$$

Let  $f = \lambda \overline{\Phi}. \lambda \bar{a}. \bar{a} \dot{\sqcup} \overline{\Phi}(\overline{\mathcal{A}}[s]\bar{a})$  be the functional in  $\overline{\mathcal{A}}[\text{\texttt{while } } e \text{\texttt{ do } } s]$ . We calculate an over-approximation of  $\alpha_{\rightarrow} \circ f \circ \gamma_{\rightarrow}$ , denoted as  $F$ , and then apply the fixed point transfer (FPT) theorem [8] on the result. Given a monotone function  $\overline{\Phi'}$ , we have:

$$\begin{aligned}
& (\alpha_{\rightarrow} \circ f \circ \gamma_{\rightarrow})\overline{\Phi'} \\
&= \alpha_{\rightarrow}(f(\lambda \bar{a}. \gamma(\overline{\Phi'}(\alpha(\bar{a})))) && \text{(by def. of } \circ \text{ and } \gamma_{\rightarrow} \text{)} \\
&= \alpha_{\rightarrow}(\lambda \bar{a}. \bar{a} \dot{\sqcup} \gamma(\overline{\Phi'}(\alpha(\overline{\mathcal{A}}[s]\bar{a})))) && \text{(by def. of } f \text{ and } \beta\text{-reduction)} \\
&= \lambda \bar{d}. \alpha(\gamma(\bar{d}) \dot{\sqcup} \gamma(\overline{\Phi'}(\alpha(\overline{\mathcal{A}}[s]\gamma(\bar{d})))) && \text{(by def. of } \alpha_{\rightarrow} \text{)} \\
&= \lambda \bar{d}. \alpha(\gamma(\bar{d}) \dot{\sqcup} \alpha(\gamma(\overline{\Phi'}(\alpha(\overline{\mathcal{A}}[s]\gamma(\bar{d})))))) && \text{(by } \alpha \text{ is a CJM)} \\
&\stackrel{\dot{=}}{=} \lambda \bar{d}. \bar{d} \dot{\sqcup} \overline{\Phi'}(\overline{\mathcal{D}}_\alpha[s]\bar{d}) && \text{(by IH; and } \alpha \circ \gamma \text{ is reductive, twice)} \\
&= F\overline{\Phi'}
\end{aligned}$$

Thus, we obtain  $F = \lambda \overline{\Phi'}. \lambda \overline{d}. \overline{d} \dot{\sqcup} \overline{\Phi'}(\overline{\mathcal{D}}_\alpha[s]\overline{d})$ . Since  $\overline{\Phi'}$  and  $\overline{\mathcal{D}}_\alpha$  are monotone,  $F$  is also monotone. We now have:

$$\begin{aligned}
& (\alpha \circ \overline{\mathcal{A}}[\text{while } e \text{ do } s] \circ \gamma)(\overline{d}) \\
&= \alpha(\text{lfp } f(\gamma(\overline{d}))) && \text{(by def. of } \overline{\mathcal{A}} \text{ in Fig. 2)} \\
&= \alpha_{\rightarrow}(\text{lfp } f)(\overline{d}) && \text{(by def. of } \alpha_{\rightarrow}) \\
&\stackrel{\cdot}{=} (\text{lfp } F)\overline{d} && \text{(by fixed point transfer (FPT) theorem)} \\
&= \overline{\mathcal{D}}_\alpha[\text{while } e \text{ do } s]\overline{d} && \text{(by def. of } \overline{\mathcal{D}} \text{ in Fig. 5)}
\end{aligned}$$

## C Appendix: Helper Lemmas

**Lemma 1.**  $\forall \alpha \in \text{Abs} : \alpha(\prod_{k \in \mathbb{K}} n) = \prod_{k' \in \alpha(\mathbb{K})} n$

*Proof.* By induction on the structure of  $\alpha$ .

**Case  $\alpha^{\text{join}}$ :**

$$\begin{aligned}
& \alpha^{\text{join}}(\prod_{k \in \mathbb{K}} n) \\
&= (\bigsqcup_{k \in \mathbb{K}} n) && \text{(by def. of } \alpha^{\text{join}}) \\
&= \prod_{k' \in \alpha^{\text{join}}(\mathbb{K})} n && \text{(by def. of } \alpha^{\text{join}}(\mathbb{K}))
\end{aligned}$$

**Case  $\alpha_\varphi^{\text{proj}}$ :**

$$\begin{aligned}
& \alpha_\varphi^{\text{proj}}(\prod_{k \in \mathbb{K}} n) \\
&= \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} n && \text{(by def. of } \alpha_\varphi^{\text{proj}}) \\
&= \prod_{k' \in \alpha_\varphi^{\text{proj}}(\mathbb{K})} n && \text{(by def. of } \alpha_\varphi^{\text{proj}}(\mathbb{K}))
\end{aligned}$$

**Case  $\alpha_1 \otimes \alpha_2$ :**

$$\begin{aligned}
& \alpha_1 \otimes \alpha_2(\prod_{k \in \mathbb{K}} n) \\
&= \alpha_1(\prod_{k \in \mathbb{K}} n) \times \alpha_2(\prod_{k \in \mathbb{K}} n) && \text{(by def. of } \alpha_1 \otimes \alpha_2) \\
&= (\prod_{k' \in \alpha_1(\mathbb{K})} n) \times (\prod_{k' \in \alpha_2(\mathbb{K})} n) && \text{(by IH, twice)} \\
&= \prod_{k' \in \alpha_1 \cup \alpha_2(\mathbb{K})} n && \text{(by def. of } \overline{x_1} \times \overline{x_2}) \\
&= \prod_{k' \in \alpha_1 \otimes \alpha_2(\mathbb{K})} n && \text{(by def. of } \alpha_1 \otimes \alpha_2(\mathbb{K}))
\end{aligned}$$

**Case  $\alpha_2 \circ \alpha_1$ :**

$$\begin{aligned}
& \alpha_2 \circ \alpha_1 \left( \prod_{k \in \mathbb{K}} n \right) \\
&= \alpha_2 \left( \alpha_1 \left( \prod_{k \in \mathbb{K}} n \right) \right) && \text{(by def. of } \circ \text{)} \\
&= \alpha_2 \left( \prod_{k' \in \alpha_1(\mathbb{K})} n \right) && \text{(by IH)} \\
&= \prod_{k'' \in \alpha_2(\alpha_1(\mathbb{K}))} n && \text{(by IH)} \\
&= \prod_{k'' \in \alpha_2 \circ \alpha_1(\mathbb{K})} n && \text{(by def. of } \alpha_2 \circ \alpha_1(\mathbb{K}) \text{)}
\end{aligned}$$

**Lemma 2.**

$$\begin{aligned}
& \forall \alpha \in Abs, \psi, \theta \in FeatExp, \overline{a_1}, \overline{a_2} \in \mathbb{A}^{\mathbb{K}} : \\
& \alpha \left( \prod_{k \in \mathbb{K}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} \right) \\
& \quad \sqsubseteq \prod_{k' \in \alpha(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha(\overline{a_1})) \sqcup \pi_{k'}(\alpha(\overline{a_2})) & \text{if } sat(k' \wedge \theta) \wedge sat(k' \wedge \neg \theta) \\ \pi_{k'}(\alpha(\overline{a_2})) & \text{if } k' \models \neg \theta \end{cases}
\end{aligned}$$

*Proof.* By induction on the structure of  $\alpha$ .

Case  $\alpha^{\text{join}}$ :

$$\begin{aligned}
& \alpha^{\text{join}} \left( \prod_{k \in \mathbb{K}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} \right) \\
&= \left( \sqcup_{k \in \mathbb{K}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} \right) \quad (\text{by def. of } \alpha^{\text{join}}) \\
&= \left( \begin{cases} \sqcup_{k \in \mathbb{K}} \pi_k(\overline{a_1}) & \text{if } \bigvee_{k \in \mathbb{K}} k \models \theta \\ \sqcup_{\{k \in \mathbb{K} \mid k \models \theta\}} \pi_k(\overline{a_1}) \sqcup \sqcup_{\{k \in \mathbb{K} \mid k \not\models \theta\}} \pi_k(\overline{a_2}) & \text{if } \text{sat}(\bigvee_{k \in \mathbb{K}} k \wedge \theta) \wedge \text{sat}(\bigvee_{k \in \mathbb{K}} k \wedge \neg \theta) \\ \sqcup_{k \in \mathbb{K}} \pi_k(\overline{a_2}) & \text{if } \bigvee_{k \in \mathbb{K}} k \models \neg \theta \end{cases} \right) \quad (\text{by def. of } \pi_k \text{ and } \sqcup) \\
&\stackrel{\cdot}{=} \left( \begin{cases} \sqcup_{k \in \mathbb{K}} \pi_k(\overline{a_1}) & \text{if } \bigvee_{k \in \mathbb{K}} k \models \theta \\ \sqcup_{k \in \mathbb{K}} \pi_k(\overline{a_1}) \sqcup \sqcup_{k \in \mathbb{K}} \pi_k(\overline{a_2}) & \text{if } \text{sat}(\bigvee_{k \in \mathbb{K}} k \wedge \theta) \wedge \text{sat}(\bigvee_{k \in \mathbb{K}} k \wedge \neg \theta) \\ \sqcup_{k \in \mathbb{K}} \pi_k(\overline{a_2}) & \text{if } \bigvee_{k \in \mathbb{K}} k \models \neg \theta \end{cases} \right) \quad (\text{by def. of } \pi_k \text{ and } \sqcup) \\
&= \left( \begin{cases} \alpha^{\text{join}}(\overline{a_1}) & \text{if } \bigvee_{k \in \mathbb{K}} k \models \theta \\ \alpha^{\text{join}}(\overline{a_1}) \sqcup \alpha^{\text{join}}(\overline{a_2}) & \text{if } \text{sat}(\bigvee_{k \in \mathbb{K}} k \wedge \theta) \wedge \text{sat}(\bigvee_{k \in \mathbb{K}} k \wedge \neg \theta) \\ \alpha^{\text{join}}(\overline{a_2}) & \text{if } \bigvee_{k \in \mathbb{K}} k \models \neg \theta \end{cases} \right) \quad (\text{by def. of } \alpha^{\text{join}})
\end{aligned}$$

We provide an example confirming that the above relation is not equality. Let  $\mathbb{K} = \{A \wedge B, A \wedge \neg B\}$ ,  $\overline{a_1} = ([x \mapsto 2], [x \mapsto 4])$ , and  $\overline{a_2} = ([x \mapsto 6], [x \mapsto 2])$ . For  $\overline{a} = \prod_{k \in \mathbb{K}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models B \\ \pi_k(\overline{a_2}) & \text{if } k \not\models B \end{cases}$ , we have  $\overline{a} = ([x \mapsto 2], [x \mapsto 2])$ . Then  $\alpha^{\text{join}}(\overline{a}) = ([x \mapsto 2])$ . On the other hand,  $\alpha^{\text{join}}(\overline{a_1}) \sqcup \alpha^{\text{join}}(\overline{a_2}) = ([x \mapsto \top])$ .

**Case  $\alpha_\varphi^{\text{proj}}$ :**

$$\begin{aligned}
& \alpha_\varphi^{\text{proj}} \left( \prod_{k \in \mathbb{K}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} \right) \\
&= \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} && \text{(by def. of } \alpha_\varphi^{\text{proj}} \text{)} \\
&= \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} \begin{cases} \pi_k(\alpha_\varphi^{\text{proj}}(\overline{a_1})) & \text{if } k \models \theta \\ \pi_k(\alpha_\varphi^{\text{proj}}(\overline{a_2})) & \text{if } k \not\models \theta \end{cases} && \text{(by def. of } \pi_k \text{ and } \alpha_\varphi^{\text{proj}} \text{)} \\
&= \prod_{k' \in \alpha_\varphi^{\text{proj}}(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_\varphi^{\text{proj}}(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha_\varphi^{\text{proj}}(\overline{a_2})) & \text{if } k' \not\models \theta \end{cases} && \text{(by def. of } \alpha_\varphi^{\text{proj}} \text{)} \\
&\stackrel{\cdot}{\sqsubseteq} \prod_{k' \in \alpha_\varphi^{\text{proj}}(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_\varphi^{\text{proj}}(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha_\varphi^{\text{proj}}(\overline{a_1})) \sqcup \pi_{k'}(\alpha_\varphi^{\text{proj}}(\overline{a_2})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg\theta) \\ \pi_{k'}(\alpha_\varphi^{\text{proj}}(\overline{a_2})) & \text{if } k' \models \neg\theta \end{cases} && \text{(by def. of } \stackrel{\cdot}{\sqsubseteq} \text{ and } \sqcup \text{)}
\end{aligned}$$

**Case  $\alpha_1 \otimes \alpha_2$ :**

$$\begin{aligned}
& \alpha_1 \otimes \alpha_2 \left( \prod_{k \in \mathbb{K}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} \right) \\
&= \alpha_1 \left( \prod_{k \in \mathbb{K}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} \right) \times \alpha_2 \left( \prod_{k \models \psi} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} \right) \\
&\quad \text{(by def. of } \alpha_1 \otimes \alpha_2) \\
&\stackrel{\sqsubseteq}{=} \prod_{k' \in \alpha_1(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_1(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha_1(\overline{a_1})) \sqcup \pi_{k'}(\alpha_1(\overline{a_2})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\alpha_1(\overline{a_2})) & \text{if } k' \models \neg \theta \end{cases} \\
&\quad \times \prod_{k' \in \alpha_2(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_2(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha_2(\overline{a_1})) \sqcup \pi_{k'}(\alpha_2(\overline{a_2})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\alpha_2(\overline{a_2})) & \text{if } k' \models \neg \theta \end{cases} \\
&\quad \text{(by IH, twice)} \\
&= \prod_{k' \in \alpha_1 \cup \alpha_2(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_1(\overline{a_1}) \times \alpha_2(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}((\alpha_1(\overline{a_1}) \times \alpha_2(\overline{a_1})) \sqcup (\alpha_1(\overline{a_2}) \times \alpha_2(\overline{a_2}))) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\alpha_1(\overline{a_2}) \times \alpha_2(\overline{a_2})) & \text{if } k' \models \neg \theta \end{cases} \\
&\quad \text{(by def. of } \overline{x_1} \times \overline{x_2}) \\
&= \prod_{k' \in \alpha_1 \otimes \alpha_2(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_1 \otimes \alpha_2(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha_1 \otimes \alpha_2(\overline{a_1})) \sqcup \pi_{k'}(\alpha_1 \otimes \alpha_2(\overline{a_2})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\alpha_1 \otimes \alpha_2(\overline{a_2})) & \text{if } k' \models \neg \theta \end{cases} \\
&\quad \text{(by def. of } \overline{x_1} \times \overline{x_2}, \text{ and } \alpha_1 \otimes \alpha_2)
\end{aligned}$$

**Case  $\alpha_2 \circ \alpha_1$ :**

$$\begin{aligned}
& \alpha_2 \circ \alpha_1 \left( \prod_{k \in \mathbb{K}} \begin{cases} \pi_k(\overline{a_1}) & \text{if } k \models \theta \\ \pi_k(\overline{a_2}) & \text{if } k \not\models \theta \end{cases} \right) \\
& \stackrel{\dot{=}}{=} \alpha_2 \left( \prod_{k' \in \alpha_1(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_1(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha_1(\overline{a_1})) \sqcup \pi_{k'}(\alpha_1(\overline{a_2})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg\theta) \\ \pi_{k'}(\alpha_1(\overline{a_2})) & \text{if } k' \models \neg\theta \end{cases} \right) \quad (\text{by IH}) \\
& = \alpha_2 \left( \left( \prod_{k' \in \alpha_1(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_1(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha_1(\overline{a_2})) & \text{if } k' \not\models \theta \end{cases} \right) \sqcup \left( \prod_{k' \in \alpha_1(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_1(\overline{a_1})) & \text{if } k' \not\models \neg\theta \\ \pi_{k'}(\alpha_1(\overline{a_2})) & \text{if } k' \models \neg\theta \end{cases} \right) \right) \\
& \quad (\text{by def. of } \sqcup \text{ and } \not\models) \\
& = \alpha_2 \left( \prod_{k' \in \alpha_1(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_1(\overline{a_1})) & \text{if } k' \models \theta \\ \pi_{k'}(\alpha_1(\overline{a_2})) & \text{if } k' \not\models \theta \end{cases} \right) \sqcup \alpha_2 \left( \prod_{k' \in \alpha_1(\mathbb{K})} \begin{cases} \pi_{k'}(\alpha_1(\overline{a_1})) & \text{if } k' \not\models \neg\theta \\ \pi_{k'}(\alpha_1(\overline{a_2})) & \text{if } k' \models \neg\theta \end{cases} \right) \\
& \quad (\text{by } \alpha_2 \text{ is CJM}) \\
& \stackrel{\dot{=}}{=} \prod_{k'' \in \alpha_2(\alpha_1(\mathbb{K}))} \begin{cases} \pi_{k''}(\alpha_2(\alpha_1(\overline{a_1}))) & \text{if } k'' \models \theta \\ \pi_{k''}(\alpha_2(\alpha_1(\overline{a_1}))) \sqcup \pi_{k''}(\alpha_2(\alpha_1(\overline{a_2}))) & \text{if } \text{sat}(k'' \wedge \theta) \wedge \text{sat}(k'' \wedge \neg\theta) \\ \pi_{k''}(\alpha_2(\alpha_1(\overline{a_2}))) & \text{if } k'' \models \neg\theta \end{cases} \\
& \sqcup \prod_{k'' \in \alpha_2(\alpha_1(\mathbb{K}))} \begin{cases} \pi_{k''}(\alpha_2(\alpha_1(\overline{a_1}))) & \text{if } k'' \models \theta \\ \pi_{k''}(\alpha_2(\alpha_1(\overline{a_1}))) \sqcup \pi_{k''}(\alpha_2(\alpha_1(\overline{a_2}))) & \text{if } \text{sat}(k'' \wedge \theta) \wedge \text{sat}(k'' \wedge \neg\theta) \\ \pi_{k''}(\alpha_2(\alpha_1(\overline{a_2}))) & \text{if } k'' \models \neg\theta \end{cases} \\
& \quad (\text{by IH; twice}) \\
& = \prod_{k'' \in \alpha_2 \circ \alpha_1(\mathbb{K})} \begin{cases} \pi_{k''}(\alpha_2 \circ \alpha_1(\overline{a_1})) & \text{if } k'' \models \theta \\ \pi_{k''}(\alpha_2 \circ \alpha_1(\overline{a_1})) \sqcup \pi_{k''}(\alpha_2 \circ \alpha_1(\overline{a_2})) & \text{if } \text{sat}(k'' \wedge \theta) \wedge \text{sat}(k'' \wedge \neg\theta) \\ \pi_{k''}(\alpha_2 \circ \alpha_1(\overline{a_2})) & \text{if } k'' \models \neg\theta \end{cases} \\
& \quad (\text{by def. of } \alpha_2 \circ \alpha_1)
\end{aligned}$$

**Lemma 3.**  $\forall \alpha \in Abs, \overline{v_1}, \overline{v_2} \in Const^{\mathbb{K}} : \alpha(\overline{v_1} \hat{\oplus} \overline{v_2}) \stackrel{\dot{=}}{=} \alpha(\overline{v_1}) \hat{\oplus} \alpha(\overline{v_2})$

*Proof.* By induction on the structure of  $\alpha$ .

**Case  $\alpha^{\text{join}}$ :**

$$\begin{aligned}
& \alpha^{\text{join}}(\overline{v_1} \hat{\oplus} \overline{v_2}) \\
& = \bigsqcup_{k \in \mathbb{K}} \pi_k(\overline{v_1} \hat{\oplus} \overline{v_2}) \quad (\text{by def. of } \alpha^{\text{join}}) \\
& = \bigsqcup_{k \in \mathbb{K}} (\pi_k(\overline{v_1}) \hat{\oplus} \pi_k(\overline{v_2})) \quad (\text{by def. of } \pi_k \text{ and } \hat{\oplus}) \\
& \stackrel{\dot{=}}{=} (\bigsqcup_{k \in \mathbb{K}} \pi_k(\overline{v_1})) \hat{\oplus} (\bigsqcup_{k \in \mathbb{K}} \pi_k(\overline{v_2})) \quad (\text{by def. of } \bigsqcup \text{ and } \hat{\oplus}) \\
& = \alpha^{\text{join}}(\overline{v_1}) \hat{\oplus} \alpha^{\text{join}}(\overline{v_2}) \quad (\text{by def. of } \alpha^{\text{join}})
\end{aligned}$$

We provide an example confirming that the above relation is not equality. Let  $\overline{v}_1 = (5, 2)$ ,  $\overline{v}_2 = (2, 5)$ , and  $\oplus = +$ . Then  $\alpha^{\text{join}}((5, 2) \hat{\oplus} (2, 5)) = \alpha^{\text{join}}((7, 7)) = 7$ . On the other hand,  $\alpha^{\text{join}}((5, 2)) = \top$ ,  $\alpha^{\text{join}}((2, 5)) = \top$ , and  $\top \hat{+} \top = \top$ .

**Case  $\alpha_\varphi^{\text{proj}}$ :**

$$\begin{aligned}
& \alpha_\varphi^{\text{proj}}(\overline{v}_1 \hat{\oplus} \overline{v}_2) \\
&= \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} \pi_k(\overline{v}_1 \hat{\oplus} \overline{v}_2) && \text{(by def. of } \alpha_\varphi^{\text{proj}}\text{)} \\
&= \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} (\pi_k(\overline{v}_1) \hat{\oplus} \pi_k(\overline{v}_2)) && \text{(by def. of } \pi_k \text{ and } \hat{\oplus}\text{)} \\
&= \left( \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} \pi_k(\overline{v}_1) \right) \hat{\oplus} \left( \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} \pi_k(\overline{v}_2) \right) && \text{(by def. of } \prod \text{ and } \hat{\oplus}\text{)} \\
&= \alpha_\varphi^{\text{proj}}(\overline{v}_1) \hat{\oplus} \alpha_\varphi^{\text{proj}}(\overline{v}_2) && \text{(by def. of } \alpha_\varphi^{\text{proj}}\text{)}
\end{aligned}$$

**Case  $\alpha_1 \otimes \alpha_2$ :**

$$\begin{aligned}
& \alpha_1 \otimes \alpha_2(\overline{v}_1 \hat{\oplus} \overline{v}_2) \\
&= \alpha_1(\overline{v}_1 \hat{\oplus} \overline{v}_2) \times \alpha_2(\overline{v}_1 \hat{\oplus} \overline{v}_2) && \text{(by def. of } \alpha_1 \otimes \alpha_2\text{)} \\
&\sqsubseteq (\alpha_1(\overline{v}_1) \hat{\oplus} \alpha_1(\overline{v}_2)) \times (\alpha_2(\overline{v}_1) \hat{\oplus} \alpha_2(\overline{v}_2)) && \text{(by IH, twice)} \\
&= (\alpha_1(\overline{v}_1) \times \alpha_2(\overline{v}_1)) \hat{\oplus} (\alpha_1(\overline{v}_2) \times \alpha_2(\overline{v}_2)) && \text{(by def. of } \times \text{ and } \hat{\oplus}\text{)} \\
&= \alpha_1 \otimes \alpha_2(\overline{v}_1) \hat{\oplus} \alpha_1 \otimes \alpha_2(\overline{v}_2) && \text{(by def. of } \alpha_1 \otimes \alpha_2\text{)}
\end{aligned}$$

**Case  $\alpha_2 \circ \alpha_1$ :**

$$\begin{aligned}
& \alpha_2 \circ \alpha_1(\overline{v}_1 \hat{\oplus} \overline{v}_2) \\
&= \alpha_2(\alpha_1(\overline{v}_1 \hat{\oplus} \overline{v}_2)) && \text{(by def. of } \circ\text{)} \\
&\sqsubseteq \alpha_2(\alpha_1(\overline{v}_1) \hat{\oplus} \alpha_1(\overline{v}_2)) && \text{(by IH)} \\
&\sqsubseteq \alpha_2(\alpha_1(\overline{v}_1)) \hat{\oplus} \alpha_2(\alpha_1(\overline{v}_2)) && \text{(by IH)} \\
&= \alpha_2 \circ \alpha_1(\overline{v}_1) \hat{\oplus} \alpha_2 \circ \alpha_1(\overline{v}_2) && \text{(by def. of } \alpha_2 \circ \alpha_1\text{)}
\end{aligned}$$

We define  $\overline{a}[\mathbf{x} \mapsto \overline{v}]$  to mean a tuple that is as  $\overline{a}$  except that in each its component the variable  $\mathbf{x}$  is mapped to the corresponding component of the tuple  $\overline{v}$ .

**Lemma 4.**  $\forall \alpha \in Abs, \overline{a} \in \mathbb{A}^{\mathbb{K}}, \overline{v} \in Const^{\mathbb{K}} : \alpha(\overline{a}[\mathbf{x} \mapsto \overline{v}]) = \alpha(\overline{a})[\mathbf{x} \mapsto \alpha(\overline{v})]$

*Proof.* By induction on the structure of  $\alpha$ .



**Case  $\alpha^{\text{join}}$ :**

$$\begin{aligned}
& \alpha^{\text{join}}(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}]) \\
&= \bigsqcup_{k \in \mathbb{K}} \pi_k(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}]) && \text{(by def. of } \alpha^{\text{join}}\text{)} \\
&= \bigsqcup_{k \in \mathbb{K}} (\pi_k(\bar{a})[\mathbf{x} \mapsto \pi_k(\bar{v})]) && \text{(by def. of } \pi_k \text{ and } \dot{\mapsto}\text{)} \\
&= (\bigsqcup_{k \in \mathbb{K}} \pi_k(\bar{a}))[\mathbf{x} \mapsto \bigsqcup_{k \in \mathbb{K}} \pi_k(\bar{v})] && \text{(by def. of } \bigsqcup \text{ and } \mapsto\text{)} \\
&= \alpha^{\text{join}}(\bar{a})[\mathbf{x} \mapsto \alpha^{\text{join}}(\bar{v})] && \text{(by def. of } \alpha^{\text{join}}\text{)}
\end{aligned}$$

**Case  $\alpha_\varphi^{\text{proj}}$ :**

$$\begin{aligned}
& \alpha_\varphi^{\text{proj}}(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}]) \\
&= \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} \pi_k(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}]) && \text{(by def. of } \alpha_\varphi^{\text{proj}}\text{)} \\
&= \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} (\pi_k(\bar{a})[\mathbf{x} \mapsto \pi_k(\bar{v})]) && \text{(by def. of } \pi_k \text{ and } \dot{\mapsto}\text{)} \\
&= \left( \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} \pi_k(\bar{a}) \right) [\mathbf{x} \dot{\mapsto} \prod_{\{k \in \mathbb{K} \mid k \models \varphi\}} \pi_k(\bar{v})] && \text{(by def. of } \prod \text{ and } \dot{\mapsto}\text{)} \\
&= \alpha_\varphi^{\text{proj}}(\bar{a})[\mathbf{x} \dot{\mapsto} \alpha_\varphi^{\text{proj}}(\bar{v})] && \text{(by def. of } \alpha_\varphi^{\text{proj}}\text{)}
\end{aligned}$$

**Case  $\alpha_1 \otimes \alpha_2$ :**

$$\begin{aligned}
& \alpha_1 \otimes \alpha_2(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}]) \\
&= \alpha_1(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}]) \times \alpha_2(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}]) && \text{(by def. of } \alpha_1 \otimes \alpha_2\text{)} \\
&= \alpha_1(\bar{a})[\mathbf{x} \dot{\mapsto} \alpha_1(\bar{v})] \times \alpha_2(\bar{a})[\mathbf{x} \dot{\mapsto} \alpha_2(\bar{v})] && \text{(by IH, twice)} \\
&= (\alpha_1(\bar{a}) \times \alpha_2(\bar{a}))[\mathbf{x} \dot{\mapsto} \alpha_1(\bar{v}) \times \alpha_2(\bar{v})] && \text{(by def. of } \times \text{ and } \dot{\mapsto}\text{)} \\
&= \alpha_1 \otimes \alpha_2(\bar{a})[\mathbf{x} \dot{\mapsto} \alpha_1 \otimes \alpha_2(\bar{v})] && \text{(by def. of } \alpha_1 \otimes \alpha_2\text{)}
\end{aligned}$$

**Case  $\alpha_2 \circ \alpha_1$ :**

$$\begin{aligned}
& \alpha_2 \circ \alpha_1(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}]) \\
&= \alpha_2(\alpha_1(\bar{a}[\mathbf{x} \dot{\mapsto} \bar{v}])) && \text{(by def. of } \alpha_2 \circ \alpha_1\text{)} \\
&= \alpha_2(\alpha_1(\bar{a})[\mathbf{x} \dot{\mapsto} \alpha_1(\bar{v})]) && \text{(by IH)} \\
&= \alpha_2(\alpha_1(\bar{a}))[\mathbf{x} \dot{\mapsto} \alpha_2(\alpha_1(\bar{v}))] && \text{(by IH)} \\
&= \alpha_2 \circ \alpha_1(\bar{a})[\mathbf{x} \dot{\mapsto} \alpha_2 \circ \alpha_1(\bar{v})] && \text{(by def. of } \alpha_2 \circ \alpha_1\text{)}
\end{aligned}$$

## D Appendix: Monotonicity of Abstracted Analyses

**Lemma 5** ( $\overline{\mathcal{D}'}_\alpha \llbracket e \rrbracket$  is monotone).

$$\forall e \in \text{Exp}, \alpha \in \text{Abs}, \bar{d}, \bar{d}' \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)}. \bar{d} \sqsubseteq \bar{d}' \implies \overline{\mathcal{D}'}_\alpha \llbracket e \rrbracket \bar{d} \sqsubseteq \overline{\mathcal{D}'}_\alpha \llbracket e \rrbracket \bar{d}'$$

*Proof.* Let  $e$ ,  $\alpha$ , and  $\bar{d} \sqsubseteq \bar{d}'$  be given. We proceed by structural induction on  $e$ .

**Case  $n$ :**

$$\overline{\mathcal{D}}'_\alpha \llbracket n \rrbracket \bar{d} = \prod_{k' \in \alpha(\mathbb{K}_\psi)} n = \overline{\mathcal{D}}'_\alpha \llbracket n \rrbracket \bar{d}'$$

**Case  $\mathbf{x}$ :**

$$\begin{aligned} \overline{\mathcal{D}}'_\alpha \llbracket \mathbf{x} \rrbracket \bar{d} &= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\bar{d})(\mathbf{x}) && \text{(by def. of } \overline{\mathcal{D}}'_\alpha) \\ &\sqsubseteq \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\bar{d}')(\mathbf{x}) && \text{(by } \bar{d} \dot{\sqsubseteq} \bar{d}') \\ &= \overline{\mathcal{D}}'_\alpha \llbracket \mathbf{x} \rrbracket \bar{d}' && \text{(by def. of } \overline{\mathcal{D}}'_\alpha) \end{aligned}$$

**Case  $e_0 \oplus e_1$ :**

$$\begin{aligned} \overline{\mathcal{D}}'_\alpha \llbracket e_0 \oplus e_1 \rrbracket \bar{d} &= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\overline{\mathcal{D}}'_\alpha \llbracket e_0 \rrbracket \bar{d}) \hat{\oplus} \pi_{k'}(\overline{\mathcal{D}}'_\alpha \llbracket e_1 \rrbracket \bar{d}) && \text{(by def. of } \overline{\mathcal{D}}'_\alpha) \\ &\sqsubseteq \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\overline{\mathcal{D}}'_\alpha \llbracket e_0 \rrbracket \bar{d}') \hat{\oplus} \pi_{k'}(\overline{\mathcal{D}}'_\alpha \llbracket e_1 \rrbracket \bar{d}') && \text{(by IH; and } \bar{d} \dot{\sqsubseteq} \bar{d}') \\ &= \overline{\mathcal{D}}'_\alpha \llbracket e_0 \oplus e_1 \rrbracket \bar{d}' && \text{(by def. of } \overline{\mathcal{D}}'_\alpha) \end{aligned}$$

**Lemma 6** ( $\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket$  is monotone).

$$\forall s \in Stm, \alpha \in Abs, \bar{d}, \bar{d}' \in \mathbb{A}^{\alpha(\mathbb{K}_\psi)}. \bar{d} \dot{\sqsubseteq} \bar{d}' \implies \overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \bar{d} \dot{\sqsubseteq} \overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \bar{d}'$$

*Proof.* Let  $s$ ,  $\alpha$ , and  $\bar{d} \dot{\sqsubseteq} \bar{d}'$  be given. We proceed by structural induction on  $s$ .

**Case skip:**

$$\overline{\mathcal{D}}_\alpha \llbracket \text{skip} \rrbracket \bar{d} = \bar{d} \dot{\sqsubseteq} \bar{d}' = \overline{\mathcal{D}}_\alpha \llbracket \text{skip} \rrbracket \bar{d}' \quad \text{(by def. of } \overline{\mathcal{D}}_\alpha)$$

**Case  $\mathbf{x} := e$ :**

$$\begin{aligned} \overline{\mathcal{D}}_\alpha \llbracket \mathbf{x} := e \rrbracket \bar{d} &= \prod_{k' \in \alpha(\mathbb{K}_\psi)} (\pi_{k'}(\bar{d}))[\mathbf{x} \mapsto \pi_{k'}(\overline{\mathcal{D}}'_\alpha \llbracket e \rrbracket \bar{d})] && \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\ &\dot{\sqsubseteq} \prod_{k' \in \alpha(\mathbb{K}_\psi)} (\pi_{k'}(\bar{d}'))[\mathbf{x} \mapsto \pi_{k'}(\overline{\mathcal{D}}'_\alpha \llbracket e \rrbracket \bar{d}')] && \text{(by } \bar{d} \dot{\sqsubseteq} \bar{d}' \text{ and Lemma 5)} \\ &= \overline{\mathcal{D}}_\alpha \llbracket \mathbf{x} := e \rrbracket \bar{d}' && \text{(by def. of } \overline{\mathcal{D}}_\alpha) \end{aligned}$$

**Case  $s_0 ; s_1$ :**

$$\begin{aligned} \overline{\mathcal{D}}_\alpha \llbracket s_0 ; s_1 \rrbracket \bar{d} &= \overline{\mathcal{D}}_\alpha \llbracket s_1 \rrbracket (\overline{\mathcal{D}}_\alpha \llbracket s_0 \rrbracket \bar{d}) && \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\ &\dot{\sqsubseteq} \overline{\mathcal{D}}_\alpha \llbracket s_1 \rrbracket (\overline{\mathcal{D}}_\alpha \llbracket s_0 \rrbracket \bar{d}') && \text{(by IH, twice; and } \bar{d} \dot{\sqsubseteq} \bar{d}') \\ &= \overline{\mathcal{D}}_\alpha \llbracket s_0 ; s_1 \rrbracket \bar{d}' && \text{(by def. of } \overline{\mathcal{D}}_\alpha) \end{aligned}$$

**Case if  $e$  then  $s_0$  else  $s_1$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_\alpha \llbracket \text{if } e \text{ then } s_0 \text{ else } s_1 \rrbracket \overline{d} \\
&= \overline{\mathcal{D}}_\alpha \llbracket s_0 \rrbracket \overline{d} \sqcup \overline{\mathcal{D}}_\alpha \llbracket s_1 \rrbracket \overline{d} && \text{(by def. of } \overline{\mathcal{D}}_\alpha \text{)} \\
&\dot{\sqsubseteq} \overline{\mathcal{D}}_\alpha \llbracket s_0 \rrbracket \overline{d'} \sqcup \overline{\mathcal{D}}_\alpha \llbracket s_1 \rrbracket \overline{d'} && \text{(by IH, twice; and } \overline{d} \dot{\sqsubseteq} \overline{d'} \text{)} \\
&= \overline{\mathcal{D}}_\alpha \llbracket \text{if } e \text{ then } s_0 \text{ else } s_1 \rrbracket \overline{d'} && \text{(by def. of } \overline{\mathcal{D}}_\alpha \text{)}
\end{aligned}$$

**Case #if  $(\theta)$   $s$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_\alpha \llbracket \# \text{if } (\theta) s \rrbracket \overline{d} \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d}) & \text{if } k' \models \theta \\ \pi_{k'}(\overline{d}) \sqcup \pi_{k'}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d}) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\overline{d}) & \text{if } k' \models \neg \theta \end{cases} && \text{(by def. of } \overline{\mathcal{D}}_\alpha \text{)} \\
&\dot{\sqsubseteq} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d'}) & \text{if } k' \models \theta \\ \pi_{k'}(\overline{d'}) \sqcup \pi_{k'}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d'}) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\overline{d'}) & \text{if } k' \models \neg \theta \end{cases} && \text{(by IH, and } \overline{d} \dot{\sqsubseteq} \overline{d'} \text{)} \\
&= \overline{\mathcal{D}}_\alpha \llbracket \# \text{if } (\theta) s \rrbracket \overline{d'} && \text{(by def. of } \overline{\mathcal{D}}_\alpha \text{)}
\end{aligned}$$

**Case while  $e$  do  $s$ :** Let  $f = \lambda \overline{\Phi}. \lambda \overline{d}. \overline{d} \sqcup \overline{\Phi}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d})$  be the functional in the rule for **while  $e$  do  $s$** . First we prove that applying the functional  $f$  to a monotone function  $\overline{\Phi}$  yields a monotone function. Thus, we obtain that the functional  $f$  operates over the complete lattice of monotone functions. Let  $\overline{d} \dot{\sqsubseteq} \overline{d'}$  and a monotone function  $\overline{\Phi}$  be given. We have:

$$\begin{aligned}
& (f\overline{\Phi})\overline{d} \\
&= \overline{d} \sqcup \overline{\Phi}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d}) && \text{(by def. of } f \text{)} \\
&\dot{\sqsubseteq} \overline{d'} \sqcup \overline{\Phi}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d'}) && \text{(by IH, monotonicity of } \overline{\Phi} \text{, and } \overline{d} \dot{\sqsubseteq} \overline{d'} \text{)} \\
&= (f\overline{\Phi})\overline{d'} && \text{(by def. of } f \text{)}
\end{aligned}$$

Second we prove that the functional  $f$  itself is monotone, which guarantees that the while rule is well defined by Tarski's fixed point theorem. We extend the operator  $\dot{\sqsubseteq}$  to operate over tuples of functions:  $\overline{f} \dot{\sqsubseteq} \overline{g} = \forall \overline{x}. \overline{f}(\overline{x}) \dot{\sqsubseteq} \overline{g}(\overline{x})$ . Let monotone functions  $\overline{\Phi}$  and  $\overline{\Phi'}$  be given and  $\overline{\Phi} \dot{\sqsubseteq} \overline{\Phi'}$ .

$$\begin{aligned}
& F\overline{\Phi} \\
&= \lambda \overline{d}. \overline{d} \sqcup \overline{\Phi}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d}) && \text{(by def. of } f \text{)} \\
&\dot{\sqsubseteq} \lambda \overline{d}. \overline{d} \sqcup \overline{\Phi'}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \overline{d}) && \text{(by def. of } \dot{\sqsubseteq} \text{, and } \overline{\Phi} \dot{\sqsubseteq} \overline{\Phi'} \text{)} \\
&= F\overline{\Phi'} && \text{(by def. of } f \text{)}
\end{aligned}$$

Since the least fixed point is an element of the complete lattice of monotone functions, it is itself monotone. Given  $\bar{d} \sqsubseteq \bar{d}'$ , we have:

$$\bar{\mathcal{D}}_\alpha \llbracket \text{while } e \text{ do } s \rrbracket \bar{d} = (\text{lfp } f) \bar{d} \sqsubseteq (\text{lfp } f) \bar{d}' = \bar{\mathcal{D}}_\alpha \llbracket \text{while } e \text{ do } s \rrbracket \bar{d}'$$

which concludes this case.

## E Appendix: Abstracted Data-flow Equations

The complete list of data-flow equations for abstracted constant propagation:

$$\begin{aligned} \llbracket \text{skip} \rrbracket_{\text{out}}^\alpha &= \llbracket \text{skip} \rrbracket_{\text{in}}^\alpha \\ \forall k' \in \alpha(\mathbb{K}_\psi): \pi_{k'}(\llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{out}}^\alpha) &= \pi_{k'}(\llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{in}}^\alpha) [x \mapsto \pi_{k'}(\bar{\mathcal{D}}'_\alpha \llbracket e^{\ell_0} \rrbracket \llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{in}}^\alpha)] \\ \llbracket s_0^{\ell_0} ;^\ell s_1^{\ell_1} \rrbracket_{\text{out}}^\alpha &= \llbracket s_1^{\ell_1} \rrbracket_{\text{out}}^\alpha \\ \llbracket s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha &= \llbracket s_0^{\ell_0} \rrbracket_{\text{out}}^\alpha \\ \llbracket s_0^{\ell_0} \rrbracket_{\text{in}}^\alpha &= \llbracket s_0^{\ell_0} ;^\ell s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha \\ \llbracket \text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1} \rrbracket_{\text{out}}^\alpha &= \llbracket s_0^{\ell_0} \rrbracket_{\text{out}}^\alpha \sqcup \llbracket s_1^{\ell_1} \rrbracket_{\text{out}}^\alpha \\ \llbracket s_0^{\ell_0} \rrbracket_{\text{in}}^\alpha &= \llbracket \text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha \\ \llbracket s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha &= \llbracket \text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha \\ \llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{out}}^\alpha &= \llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha \\ \llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha &= \llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha \sqcup \llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha \\ \forall k' \in \alpha(\mathbb{K}_\psi): \pi_{k'}(\llbracket \# \text{if}^\ell(\theta) s^{\ell_0} \rrbracket_{\text{out}}^\alpha) &= \begin{cases} \pi_{k'}(\llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) & \text{if } k' \models \theta \\ \pi_{k'}(\llbracket \# \text{if}^\ell(\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \sqcup \pi_{k'}(\llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\llbracket \# \text{if}^\ell(\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) & \text{if } k' \models \neg \theta \end{cases} \\ \forall k' \in \alpha(\mathbb{K}_\psi): \pi_{k'}(\llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha) &= \pi_{k'}(\llbracket \# \text{if}^\ell(\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \quad \text{if } (k' \wedge \theta \text{ is sat}) \end{aligned}$$

We can derive data-flow equations for expressions as well, but for brevity we refer directly to  $\bar{\mathcal{D}}'_\alpha \llbracket e \rrbracket$  function.

**Theorem 7 (Soundness of Abstracted Data-Flow Equations).** *For all  $s \in \text{Stm}$  and  $\alpha \in \text{Abs}$ , such that  $\llbracket s^\ell \rrbracket_{\text{in}}^\alpha$  and  $\llbracket s^\ell \rrbracket_{\text{out}}^\alpha$  satisfy the data-flow equations in Fig. 6, it holds:*

$$\bar{\mathcal{D}}_\alpha \llbracket s^\ell \rrbracket (\llbracket s^\ell \rrbracket_{\text{in}}^\alpha) \sqsubseteq \llbracket s^\ell \rrbracket_{\text{out}}^\alpha$$

*Proof.* The proof is by structural induction on  $s^\ell$ .

**Case  $\text{skip}^\ell$ :**

$$\begin{aligned} &\bar{\mathcal{D}}_\alpha \llbracket \text{skip}^\ell \rrbracket (\llbracket \text{skip}^\ell \rrbracket_{\text{in}}^\alpha) \\ &= \llbracket \text{skip}^\ell \rrbracket_{\text{in}}^\alpha && \text{(by def. of } \bar{\mathcal{D}}_\alpha) \\ &= \llbracket \text{skip}^\ell \rrbracket_{\text{out}}^\alpha && \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha \text{ and } \llbracket - \rrbracket_{\text{out}}^\alpha) \end{aligned}$$

**Case  $x :=^\ell e$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_\alpha \llbracket x :=^\ell e^{\ell_0} \rrbracket (\llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{in}}^\alpha) \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} (\pi_{k'}(\llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{in}}^\alpha)) [x \mapsto \pi_{k'}(\overline{\mathcal{D}}'_\alpha \llbracket e \rrbracket \llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{in}}^\alpha)] \\
&\hspace{25em} \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \pi_{k'}(\llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{out}}^\alpha) \hspace{2em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha \text{ and } \llbracket - \rrbracket_{\text{out}}^\alpha) \\
&= \llbracket x :=^\ell e^{\ell_0} \rrbracket_{\text{out}}^\alpha
\end{aligned}$$

**Case  $s_0^{\ell_0} ;^\ell s_1^{\ell_1}$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_\alpha \llbracket s_0^{\ell_0} ;^\ell s_1^{\ell_1} \rrbracket (\llbracket s_0^{\ell_0} ;^\ell s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha) \\
&= \overline{\mathcal{D}}_\alpha \llbracket s_1^{\ell_1} \rrbracket (\overline{\mathcal{D}}_\alpha \llbracket s_0^{\ell_0} \rrbracket \llbracket s_0^{\ell_0} ;^\ell s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha) \hspace{2em} \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\
&= \overline{\mathcal{D}}_\alpha \llbracket s_1^{\ell_1} \rrbracket (\overline{\mathcal{D}}_\alpha \llbracket s_0^{\ell_0} \rrbracket (\llbracket s_0^{\ell_0} \rrbracket_{\text{in}}^\alpha)) \hspace{2em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha \text{ and } \llbracket - \rrbracket_{\text{out}}^\alpha) \\
&\dot{\subseteq} \overline{\mathcal{D}}_\alpha \llbracket s_1^{\ell_1} \rrbracket (\llbracket s_0^{\ell_0} \rrbracket_{\text{out}}^\alpha) \hspace{2em} \text{(by IH)} \\
&= \overline{\mathcal{D}}_\alpha \llbracket s_1^{\ell_1} \rrbracket (\llbracket s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha) \hspace{2em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha \text{ and } \llbracket - \rrbracket_{\text{out}}^\alpha) \\
&\dot{\subseteq} \llbracket s_1^{\ell_1} \rrbracket_{\text{out}}^\alpha \hspace{2em} \text{(by IH)} \\
&= (\llbracket s_0^{\ell_0} ;^\ell s_1^{\ell_1} \rrbracket_{\text{out}}^\alpha) \hspace{2em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha \text{ and } \llbracket - \rrbracket_{\text{out}}^\alpha)
\end{aligned}$$

**Case  $\text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1}$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_\alpha \llbracket \text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1} \rrbracket (\llbracket \text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha) \\
&= \overline{\mathcal{D}}_\alpha \llbracket s_0^{\ell_0} \rrbracket (\llbracket \text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha) \dot{\cup} \\
&\quad \overline{\mathcal{D}}_\alpha \llbracket s_1^{\ell_1} \rrbracket (\llbracket \text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha) \hspace{2em} \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\
&= \overline{\mathcal{D}}_\alpha \llbracket s_0^{\ell_0} \rrbracket (\llbracket s_0^{\ell_0} \rrbracket_{\text{in}}^\alpha) \dot{\cup} \overline{\mathcal{D}}_\alpha \llbracket s_1^{\ell_1} \rrbracket (\llbracket s_1^{\ell_1} \rrbracket_{\text{in}}^\alpha) \hspace{2em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha, \llbracket - \rrbracket_{\text{out}}^\alpha) \\
&\dot{\subseteq} \llbracket s_0^{\ell_0} \rrbracket_{\text{out}}^\alpha \dot{\cup} \llbracket s_1^{\ell_1} \rrbracket_{\text{out}}^\alpha \hspace{2em} \text{(by IH, twice)} \\
&= \llbracket \text{if}^\ell e \text{ then } s_0^{\ell_0} \text{ else } s_1^{\ell_1} \rrbracket_{\text{out}}^\alpha \hspace{2em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha, \llbracket - \rrbracket_{\text{out}}^\alpha)
\end{aligned}$$

**Case  $\# \text{if}^\ell (\theta) s^{\ell_0}$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_\alpha \llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket (\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_\alpha \llbracket s^{\ell_0} \rrbracket (\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha)) & \text{if } k' \models \theta \\ \pi_{k'}(\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \sqcup \pi_{k'}(\overline{\mathcal{D}}_\alpha \llbracket s^{\ell_0} \rrbracket (\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha)) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) & \text{if } k' \models \neg \theta \end{cases} \\
& \hspace{15em} \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\
&= \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_\alpha \llbracket s^{\ell_0} \rrbracket (\llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha)) & \text{if } k' \models \theta \\ \pi_{k'}(\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \sqcup \pi_{k'}(\overline{\mathcal{D}}_\alpha \llbracket s^{\ell_0} \rrbracket (\llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha)) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) & \text{if } k' \models \neg \theta \end{cases} \\
& \hspace{15em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha, \llbracket - \rrbracket_{\text{out}}^\alpha) \\
&\dot{\sqsubseteq} \prod_{k' \in \alpha(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) & \text{if } k' \models \theta \\ \pi_{k'}(\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \sqcup \pi_{k'}(\llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{in}}^\alpha) & \text{if } k' \models \neg \theta \end{cases} \\
& \hspace{15em} \text{(by IH)} \\
&= \llbracket \# \text{if}^\ell (\theta) s^{\ell_0} \rrbracket_{\text{out}}^\alpha \hspace{15em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha, \llbracket - \rrbracket_{\text{out}}^\alpha)
\end{aligned}$$

**Case  $\text{while}^\ell e \text{ do } s^{\ell_0}$ :** Let  $f = \lambda \overline{\mathcal{D}}. \lambda \bar{d}. \bar{d} \dot{\sqcup} \overline{\mathcal{F}}(\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket \bar{d})$  be the functional in the rule for  $\text{while } e \text{ do } s$ . We first prove by inner induction on  $n$ , that:

$$f^n(\bar{\perp})(\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\sqcup} \llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) \dot{\sqsubseteq} \llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{out}}^\alpha \quad (14)$$

for all  $n \geq 0$ , where  $\bar{\perp} = \lambda \bar{d}. \bar{\perp}$ . The base case for  $n = 0$  is straightforward. For the inductive case  $n = k + 1$ , we assume that:

$$f^k(\bar{\perp})(\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\sqcup} \llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) \dot{\sqsubseteq} \llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{out}}^\alpha$$

Then we have:

$$\begin{aligned}
& f^{k+1}(\bar{\perp})(\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\sqcup} \llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) \\
&= f^{k+1}(\bar{\perp})(\llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \hspace{10em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha, \llbracket - \rrbracket_{\text{out}}^\alpha) \\
&= f(f^k(\bar{\perp}))(\llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \hspace{10em} \text{(by def. of } f^{k+1}) \\
&= \llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\sqcup} f^k(\bar{\perp})(\overline{\mathcal{D}}_\alpha \llbracket s^{\ell_0} \rrbracket (\llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha)) \hspace{10em} \text{(by def. of } f) \\
&\dot{\sqsubseteq} \llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\sqcup} f^k(\bar{\perp})(\llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) \hspace{10em} \text{(by outer IH, monotonicity of } f^k(\bar{\perp})) \\
&\dot{\sqsubseteq} \llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\sqcup} f^k(\bar{\perp})(\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\sqcup} \llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) \\
& \hspace{15em} \text{(by monotonicity of } f^k(\bar{\perp})) \\
&\dot{\sqsubseteq} \llbracket s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\sqcup} \llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{out}}^\alpha \hspace{10em} \text{(by inner IH)} \\
&= \llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{out}}^\alpha \hspace{10em} \text{(by def. of } \llbracket - \rrbracket_{\text{in}}^\alpha, \llbracket - \rrbracket_{\text{out}}^\alpha)
\end{aligned}$$

Finally, we have:

$$\begin{aligned}
& \overline{\mathcal{D}}_\alpha \llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket (\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha) \\
&= (\text{lfp } f)(\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha) && \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\
&= (\lambda \bar{d}. \dot{\cup}_i f^i(\bar{\perp})(\bar{d}))(\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha) && \text{(by Kleene's fixed point theorem)} \\
&= \dot{\cup}_i f^i(\bar{\perp})(\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha) && (\beta\text{-reduction}) \\
&\dot{\subseteq} \dot{\cup}_i f^i(\bar{\perp})(\llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{in}}^\alpha \dot{\cup} \llbracket s^{\ell_0} \rrbracket_{\text{out}}^\alpha) && \text{(by monotonicity of } f^i(\bar{\perp})) \\
&\dot{\subseteq} \llbracket \text{while}^\ell e \text{ do } s^{\ell_0} \rrbracket_{\text{out}}^\alpha && \text{(by Eq. (14))}
\end{aligned}$$

## F Appendix: Proof that $\overline{\mathcal{D}}_\alpha \llbracket s \rrbracket$ coincides with $\overline{\mathcal{A}} \llbracket \alpha(s) \rrbracket$

*Proof.* By induction on the structure of  $\alpha \in \text{Abs}$  and  $s \in \text{Stm}$ . Apart from the **#if**-statement, for all other statements the proof is immediate from definitions of  $\overline{\mathcal{D}}_\alpha$ ,  $\overline{\mathcal{A}}$ , and  $\alpha(s)$ .

Let us consider the case of **#if** ( $\theta$ )  $s$ .

**Case  $\alpha'_{Z'}^{\text{join}}$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_{\alpha^{\text{join}}_{Z'}} \llbracket \text{\#if } (\theta) s \rrbracket \bar{d} && \text{(set of feat. is } \mathbb{F}, \text{ set of configs. is } \mathbb{K}_\psi) \\
&= \begin{cases} \overline{\mathcal{D}}_{\alpha^{\text{join}}_{Z'}} \llbracket s \rrbracket \bar{d} & \text{if } \bigvee_{k \in \mathbb{K}_\psi} k \models \theta \\ \bar{d} \dot{\cup} \overline{\mathcal{D}}_{\alpha^{\text{join}}_{Z'}} \llbracket s \rrbracket \bar{d} & \text{if } \text{sat}(\bigvee_{k \in \mathbb{K}_\psi} k \wedge \theta) \wedge \text{sat}(\bigvee_{k \in \mathbb{K}_\psi} k \wedge \neg \theta) \\ \bar{d} & \text{if } \bigvee_{k \in \mathbb{K}_\psi} k \models \neg \theta \end{cases} && \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\
&= \begin{cases} \overline{\mathcal{A}} \llbracket \alpha'_{Z'}^{\text{join}}(s) \rrbracket \bar{d} & \text{if } \bigvee_{k \in \mathbb{K}_\psi} k \models \theta \\ \bar{d} \dot{\cup} \overline{\mathcal{A}} \llbracket \alpha'_{Z'}^{\text{join}}(s) \rrbracket \bar{d} & \text{if } \text{sat}(\bigvee_{k \in \mathbb{K}_\psi} k \wedge \theta) \wedge \text{sat}(\bigvee_{k \in \mathbb{K}_\psi} k \wedge \neg \theta) \\ \bar{d} & \text{if } \bigvee_{k \in \mathbb{K}_\psi} k \models \neg \theta \end{cases} && \text{(by IH)} \\
&= \begin{cases} \overline{\mathcal{A}} \llbracket \text{\#if } (Z) \alpha'_{Z'}^{\text{join}}(s) \rrbracket \bar{d} & \text{if } \bigvee_{k \in \mathbb{K}_\psi} k \models \theta \\ \overline{\mathcal{A}} \llbracket \text{\#if } (Z) \text{ lub}(\alpha'_{Z'}^{\text{join}}(s), \text{skip}) \rrbracket \bar{d} & \text{if } \text{sat}(\bigvee_{k \in \mathbb{K}_\psi} k \wedge \theta) \wedge \text{sat}(\bigvee_{k \in \mathbb{K}_\psi} k \wedge \neg \theta) \\ \overline{\mathcal{A}} \llbracket \text{\#if } (\neg Z) \alpha'_{Z'}^{\text{join}}(s) \rrbracket \bar{d} & \text{if } \bigvee_{k \in \mathbb{K}_\psi} k \models \neg \theta \end{cases} \\
&\quad \text{(by def. of } \overline{\mathcal{A}}; \text{ renaming: set of feat. is } \{Z\}, \text{ set of configs. is } \{Z\}) \\
&= \overline{\mathcal{A}} \llbracket \alpha'_{Z'}^{\text{join}}(\text{\#if } (\theta) s) \rrbracket \bar{d} && \text{(by def. of } \overline{\mathcal{A}} \text{ and } \alpha'_{Z'}^{\text{join}}(\text{\#if } (\theta) s))
\end{aligned}$$

**Case  $\alpha_\varphi^{\text{proj}}$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_{\alpha_\varphi^{\text{proj}}}[\#\text{if } (\theta) s] \overline{d} && \text{(set of feat. is } \mathbb{F}, \text{ set of configs. is } \mathbb{K}_\psi) \\
& = \prod_{\{k \in \mathbb{K}_\psi \mid k \models \varphi\}} \begin{cases} \pi_k(\overline{\mathcal{D}}_{\alpha_\varphi^{\text{proj}}}[s] \overline{d}) & \text{if } k \models \theta \\ \pi_k(\overline{d}) \sqcup \pi_k(\overline{\mathcal{D}}_{\alpha_\varphi^{\text{proj}}}[s] \overline{d}) & \text{if } \text{sat}(k \wedge \theta) \wedge \text{sat}(k \wedge \neg \theta) \\ \pi_k(\overline{d}) & \text{if } k \models \neg \theta \end{cases} \\
& && \text{(by def. of } \overline{\mathcal{D}}_\alpha) \\
& = \prod_{\{k \in \mathbb{K}_\psi \mid k \models \varphi\}} \begin{cases} \pi_k(\overline{\mathcal{D}}_{\alpha_\varphi^{\text{proj}}}[s] \overline{d}) & \text{if } k \models \theta \\ \pi_k(\overline{d}) & \text{if } k \not\models \theta \end{cases} && \text{(since } k \text{ is a valuation)} \\
& = \prod_{\{k \in \mathbb{K}_\psi \mid k \models \varphi\}} \begin{cases} \pi_k(\overline{\mathcal{A}}[\alpha_\varphi^{\text{proj}}(s)] \overline{d}) & \text{if } k \models \theta \\ \pi_k(\overline{d}) & \text{if } k \not\models \theta \end{cases} && \text{(by IH)} \\
& = \overline{\mathcal{A}}[\#\text{if } (\theta) \alpha_\varphi^{\text{proj}}(s)] \overline{d} \\
& \text{(by def. of } \overline{\mathcal{A}}; \text{ renaming: set of feat. is } \mathbb{F}, \text{ set of configs. is } \{k \in \mathbb{K}_\psi \mid k \models \varphi\}) \\
& = \overline{\mathcal{A}}[\alpha_\varphi^{\text{proj}}(\#\text{if } (\theta) s)] \overline{d} && \text{(by def. of } \overline{\mathcal{A}} \text{ and } \alpha_\varphi^{\text{proj}}(\#\text{if } (\theta) s))
\end{aligned}$$



**Case  $\alpha_1 \otimes \alpha_2$ :**

$$\begin{aligned}
& \overline{\mathcal{D}}_{\alpha_1 \otimes \alpha_2} \llbracket \# \text{if } (\theta) \ s \rrbracket (\bar{d}) \quad (\text{set of feat. is } \mathbb{F}, \text{ set of configs. is } \mathbb{K}_\psi) \\
&= \prod_{k' \in \alpha_1 \otimes \alpha_2(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_{\alpha_1 \otimes \alpha_2} \llbracket s \rrbracket \bar{d}) & \text{if } k' \models \theta \\ \pi_{k'}(\bar{d}) \sqcup \pi_{k'}(\overline{\mathcal{D}}_{\alpha_1 \otimes \alpha_2} \llbracket s \rrbracket \bar{d}) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\bar{d}) & \text{if } k' \models \neg \theta \end{cases} \quad (\text{by def. of } \overline{\mathcal{D}}_\alpha) \\
&= \prod_{k' \in \alpha_1(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_{\alpha_1} \llbracket s \rrbracket \pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) & \text{if } k' \models \theta \\ \pi_{k'}(\pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) \sqcup \pi_{k'}(\overline{\mathcal{D}}_{\alpha_1} \llbracket s \rrbracket \pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) & \text{if } k' \models \neg \theta \end{cases} \\
&\quad \times \prod_{k' \in \alpha_2(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{D}}_{\alpha_2} \llbracket s \rrbracket \pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) & \text{if } k' \models \theta \\ \pi_{k'}(\pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) \sqcup \pi_{k'}(\overline{\mathcal{D}}_{\alpha_2} \llbracket s \rrbracket \pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) & \text{if } k' \models \neg \theta \end{cases} \quad (\text{by def. of } \pi_{\alpha_1(\mathbb{K}_\psi)}, \pi_{\alpha_2(\mathbb{K}_\psi)} \text{ and } \alpha_1 \otimes \alpha_2) \\
&= \prod_{k' \in \alpha_1(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{A}} \llbracket \alpha_1(s) \rrbracket \pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) & \text{if } k' \models \theta \\ \pi_{k'}(\pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) \sqcup \pi_{k'}(\overline{\mathcal{A}} \llbracket \alpha_1(s) \rrbracket \pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) & \text{if } k' \models \neg \theta \end{cases} \\
&\quad \times \prod_{k' \in \alpha_2(\mathbb{K}_\psi)} \begin{cases} \pi_{k'}(\overline{\mathcal{A}} \llbracket \alpha_2(s) \rrbracket \pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) & \text{if } k' \models \theta \\ \pi_{k'}(\pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) \sqcup \pi_{k'}(\overline{\mathcal{A}} \llbracket \alpha_2(s) \rrbracket \pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) & \text{if } \text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg \theta) \\ \pi_{k'}(\pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) & \text{if } k' \models \neg \theta \end{cases} \quad (\text{by IH on } \alpha) \\
&= \prod_{\bar{k}' \in \alpha_1(\mathbb{K}_\psi)} \begin{cases} \pi_{\bar{k}'}(\overline{\mathcal{A}} \llbracket \overline{\alpha_1}(s, \theta) \rrbracket \pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) & \text{if } \bar{k}' \models \overline{\alpha_1}(\theta) \\ \pi_{\bar{k}'}(\pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d})) & \text{if } \bar{k}' \not\models \overline{\alpha_1}(\theta) \end{cases} \\
&\quad \times \prod_{\bar{k}' \in \alpha_2(\mathbb{K}_\psi)} \begin{cases} \pi_{\bar{k}'}(\overline{\mathcal{A}} \llbracket \overline{\alpha_2}(s, \theta) \rrbracket \pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) & \text{if } \bar{k}' \models \overline{\alpha_2}(\theta) \\ \pi_{\bar{k}'}(\pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d})) & \text{if } \bar{k}' \not\models \overline{\alpha_2}(\theta) \end{cases} \quad (\text{by def. } \overline{\alpha_1}, \overline{\alpha_2}; \text{ renaming: to } \alpha_1 \otimes \alpha_2(\mathbb{F}), \alpha_1 \otimes \alpha_2(\mathbb{K}_\psi), \text{ See } (*)) \\
&= \overline{\mathcal{A}} \llbracket \alpha_1(\# \text{if } (\theta) \ s) \rrbracket \pi_{\alpha_1(\mathbb{K}_\psi)}(\bar{d}) \times \overline{\mathcal{A}} \llbracket \alpha_2(\# \text{if } (\theta) \ s) \rrbracket \pi_{\alpha_2(\mathbb{K}_\psi)}(\bar{d}) \quad (\text{by def. of } \overline{\mathcal{A}}, \alpha_1, \text{ and } \alpha_2) \\
&= \begin{cases} \overline{\mathcal{A}} \llbracket \# \text{if } (\overline{\alpha_1}(\theta) \vee \overline{\alpha_2}(\theta)) \ \overline{\alpha_1}(s, \theta) \rrbracket & \text{if } \overline{\alpha_1}(s, \theta) = \overline{\alpha_2}(s, \theta) \\ \overline{\mathcal{A}} \llbracket \alpha_1(\# \text{if } (\theta) \ s); \alpha_2(\# \text{if } (\theta) \ s) \rrbracket & \text{otherwise} \end{cases} \quad (\text{by def. of } \overline{\mathcal{A}}, \overline{\alpha_1}, \text{ and } \overline{\alpha_2}) \\
&= \overline{\mathcal{A}} \llbracket \alpha_1 \otimes \alpha_2(\# \text{if } (\theta) \ s) \rrbracket (\bar{d}) \quad (\text{by def. of } \alpha_1 \otimes \alpha_2(\# \text{if } (\theta) \ s))
\end{aligned}$$

(\*) Note that  $\bar{k}'$  is a renamed configuration of  $k'$ . The second case  $\text{sat}(k' \wedge \theta) \wedge \text{sat}(k' \wedge \neg\theta)$  has collapsed into the first case when  $\bar{k}' \models \bar{\alpha}_1(\theta)$  and  $\bar{\alpha}_1(s, \theta) = \text{lub}(\alpha_1(s), \text{skip})$  in the equation obtained after the renaming.

**Case  $\alpha_2 \circ \alpha_1$ :**

$$\begin{aligned}
& \bar{\mathcal{D}}_{\alpha_2 \circ \alpha_1} [\# \text{if } (\theta) \ s] (\bar{d}) \quad (\text{set of feat. is } \mathbb{F}, \text{ set of configs. is } \mathbb{K}_\psi) \\
&= \prod_{k'' \in \alpha_2 \circ \alpha_1(\mathbb{K}_\psi)} \begin{cases} \pi_{k''}(\bar{\mathcal{D}}_{\alpha_2 \circ \alpha_1} [s] \bar{d}) & \text{if } k'' \models \theta \\ \pi_{k''}(\bar{d}) \sqcup \pi_{k''}(\bar{\mathcal{D}}_{\alpha_2 \circ \alpha_1} [s] \bar{d}) & \text{if } \text{sat}(k'' \wedge \theta) \wedge \text{sat}(k'' \wedge \neg\theta) \\ \pi_{k''}(\bar{d}) & \text{if } k'' \models \neg\theta \end{cases} \quad (\text{by def. of } \bar{\mathcal{D}}_\alpha) \\
&= \prod_{k'' \in \alpha_2 \circ \alpha_1(\mathbb{K}_\psi)} \begin{cases} \pi_{k''}(\bar{\mathcal{A}}[\alpha_2 \circ \alpha_1(s)] \bar{d}) & \text{if } k'' \models \theta \\ \pi_{k''}(\bar{d}) \sqcup \pi_{k''}(\bar{\mathcal{A}}[\alpha_2 \circ \alpha_1(s)] \bar{d}) & \text{if } \text{sat}(k'' \wedge \theta) \wedge \text{sat}(k'' \wedge \neg\theta) \\ \pi_{k''}(\bar{d}) & \text{if } k'' \models \neg\theta \end{cases} \quad (\text{by IH on } s) \\
&= \prod_{\bar{k}'' \in \alpha_2 \circ \alpha_1(\mathbb{K}_\psi)} \begin{cases} \pi_{\bar{k}''}(\bar{\mathcal{A}}[\bar{\alpha}_2(\bar{\alpha}_1(s, \theta), \bar{\alpha}_1(\theta))] \bar{d}) & \text{if } \bar{k}'' \models \bar{\alpha}_2(\bar{\alpha}_1(\theta)) \\ \pi_{\bar{k}''}(\bar{d}) & \text{if } \bar{k}'' \not\models \bar{\alpha}_2(\bar{\alpha}_1(\theta)) \end{cases} \\
&\quad (\text{by def. of } \bar{\alpha}, \text{ renaming: to } \alpha_2 \circ \alpha_1(\mathbb{F}), \alpha_2 \circ \alpha_1(\mathbb{K}_\psi), \text{ See } (**)) \\
&= \bar{\mathcal{A}}[\# \text{if } (\alpha_2(\alpha_1(\theta))) \ \bar{\alpha}_2(\bar{\alpha}_1(s, \theta), \bar{\alpha}_1(\theta))] \bar{d} \quad (\text{by def. of } \bar{\mathcal{A}}) \\
&= \bar{\mathcal{A}}[\alpha_2 \circ \alpha_1(\# \text{if } (\theta) \ s)] (\bar{d}) \quad (\text{by def. of } \alpha_2 \circ \alpha_1(\# \text{if } (\theta) \ s))
\end{aligned}$$

(\*\*) Note that  $\bar{k}''$  is a renamed configuration of  $k''$ , and  $\bar{k}''$  is a valuation over  $\alpha_2 \circ \alpha_1(\mathbb{F})$ . The second case  $\text{sat}(k'' \wedge \theta) \wedge \text{sat}(k'' \wedge \neg\theta)$  has collapsed into the first case when  $\bar{k}'' \models \bar{\alpha}_2(\bar{\alpha}_1(\theta))$  and  $\bar{\alpha}_1(s, \theta)$  or  $\bar{\alpha}_2(\bar{\alpha}_1(s, \theta), \bar{\alpha}_1(\theta))$  is transformed into *lub* statement.